Empirische Erfassung und Prädiktion von Datenschutz-Verhalten beim Onlineshopping

Am Fachbereich Maschinenbau
an der Technischen Universität Darmstadt
zur
Erlangung des Grades eines
Doktor der Philosophie
genehmigte

DISSERTATION

vorgelegt von
M. Sc. Heike Märki
aus Groß-Umstadt

Berichterstatter:
Professor Dr.-Ing. Ralph Bruder
Mitberichterstatter:
Professor Dr. Christine Sutter

Tag der Einreichung: 13.11.2018
Tag der mündlichen Prüfung: 26.02.2019

Darmstadt 2019
D17

Märki, Heike: Empirische Erfassung und Prädiktion von Datenschutz-Verhalten beim Onlineshopping
Darmstadt, Technische Universität Darmstadt
Jahr der Veröffentlichung der Dissertation auf TUprints: 2019
URN: urn:nbn:de:tuda-tuprints-88727
Tag der mündlichen Prüfung: 26. Februar 2019

Danksagung

Ich persönlich bin sehr stolz auf mich, dass ich diese Arbeit zu einem erfolgreichen Ende gebracht habe. Doch gibt es eine Reihe von Personen, die maßgeblich dazu beigetragen haben und denen ich an dieser Stelle ganz herzlich dafür danken möchte.
Zu diesen gehören, Herr Professor Bruder, der im Gegensatz zu mir, wie er sagt, nie am Abschluss dieser Arbeit gezweifelt hat. Ihnen möchte ich danken für die Aufnahme in die IAD-Familie, das Vertrauen in mich und die Unterstützung jeglicher Art in den letzten Jahren. Danke auch an Frau Professor Sutter für die inhaltliche Unterstützung und die Bereitschaft den Weg der Doktorarbeit bis zum Ende mitzugehen.
Während meiner Zeit am IAD durfte ich mit sehr vielen tollen Kollegen am IAD zusammenarbeiten. Ihnen allen sei gedankt für eine großartige Gemeinschaft, unterschiedlichste Arten der Unterstützung und gegenseitige Wertschätzung. Besonders hervorgehoben seien hier die Mitglieder meiner Erfolgsteams, allen voran Marius Oberle und Katharina Rönick. Vielen Dank für nächtelange Debatten, die mich inhaltlich immer sehr viel weitergebracht haben, bei denen das leibliche Wohl aber nicht vergessen wurde. Besonders ohne Katharina wäre ich in der heißen Phase dieser Arbeit wahrscheinlich verhungert oder nervlich aus der Bahn geraten. Ich danke Dir dafür sehr!
Auch Michaela Kauer, früher Kollegin, heute Freundin, möchte ich für alles danken, was sie mir in den letzten Jahren Gutes getan hat. Mir hat das Arbeiten nie solchen Spaß gemacht, wie während unserer gemeinsamen Projekte. Du hast mich angesteckt mit Deiner Begeisterung für die Forschung und wissenschaftliches Arbeiten, hast mir inhaltlich immer weitergeholfen und mich immer als Vorbild motiviert. Ein wesentlicher Antreiber im Endspurt dieser Arbeit war für mich, Dir zu beweisen, dass es doch möglich ist unter meinen Umständen eine solche Arbeit zu Ende zu bringen. Ich bin sehr froh Dich gefunden zu haben.
Ein weiterer großer Dank geht an meine Exilgastgeber Ulrike Vedra und Olieta und Niels Mumme. Ohne die Möglichkeit mehrfach einige Tage bei Euch unterzukommen um in Ruhe und am Stück arbeiten zu können hätte ich mein Abgabeziel bestimmt nicht erreicht. Darüber hinaus habe ich mich bei Euch nicht nur wegen der tollen Bewirtung überaus wohl gefühlt. Danke dafür!
Gar nicht genug danken kann ich meinen Eltern, Mechthild und Gunther Theuerling. Ihr habt mich immer unterstützt, mir Selbstvertrauen gegeben und bei allem, in dem im ich mich versuchen wollte in meinem Rücken gestanden um mich auffangen zu können. Ich kann nur hoffen, meine Sache als Elternteil genauso gut zu machen. Und Mama, ich werde Dich wohl ewig vermissen, aber ich weiß, dass Du sehr stolz auf mich und meine kleine Familie wärst. Danke für alles!
Meinem Paps und seiner Freundin Monika van Bommel danke ich darüber hinaus für ihre Unterstützung und das liebevolle Kümmern und Bespaßen meiner Kinder, um mir das Arbeiten zu ermöglichen. Ihr macht das toll und ich bin unendlich froh, dass es Euch gibt.
Und damit komme ich zu den wichtigsten Menschen in meinem Leben, denen womöglich erst, wenn Sie selbst Eltern werden annähernd bewusst wird, wie viel sie mir bedeuten. Liebe Roja und liebe Malia, ohne es zu wissen habt ihr einen großen Teil dazu beigetragen, dass ich mir einen solch schönen Hut aufsetzen durfte. Ihr habt meinen Blick auf so Vieles verändert und erfüllt mich mit so viel Stolz, Liebe und Lebensfreude, wie ich es vorher nicht für möglich gehalten habe.
Dafür auch den größten Dank an meinen Mann Daniel! Ich bin unfassbar dankbar, den besten Mann der Welt an meiner Seite zu haben. Ich danke Dir dafür, dass Du da bist, dass Du Du bist, für unsere tollen Kinder und alles was Du immer für mich und mit mir machst.
Ohne Dich hätte ich das hier nicht geschafft!

Zusammenfassung

Personenbezogene Daten von Internetnutzern sind heutzutage ein begehrtes Gut. Aus der Erhebung, Sammlung und Speicherung dieser Daten können sich für die Nutzer unterschiedliche, auch negative Konsequenzen ergeben. Obwohl die Nutzer, wenn danach gefragt, um die Sicherheit ihrer Daten besorgt sind, lassen Nutzungsdaten von sozialen Netzwerken oder Umsatzzahlen bezüglich Onlineshopping daran zweifeln. Das Phänomen der Inkonsistenz zwischen Aussagen von Befragten zu ihrem Verhalten bezüglich des Datenschutzes wird in der Literatur *privacy paradox* genannt. Daraus ergibt sich für die Forschung in diesem Kontext die Notwendigkeit der Erfassung von tatsächlichem Verhalten, um haltbare Aussagen bezüglich Einflussfaktoren und daraus abgeleiteter Ansatzpunkte für potentielle Interventionen oder Unterstützungen machen zu können. Dabei muss der Schwierigkeit begegnet werden, das Verhalten von Nutzern in einer Risikosituation zu untersuchen, ohne diese einem tatsächlichen Risiko auszusetzen und trotzdem eine möglichst reale Situation zu schaffen.
Initiales Ziel der Arbeit ist daher die Identifikation einer geeigneten Möglichkeit zur empirischen Erfassung tatsächlichen Datenschutz-Verhaltens beim Onlineshopping. Weitere Ziele stellen die Übersetzung des erfassten Verhaltens in aussagekräftige Daten und die Ermittlung signifikanter Prädiktoren dar.
Zur notwendigen Operationalisierung des Konstruktes *tatsächliches Datenschutz-Verhalten beim Onlineshopping* wird im ersten Schritt eine Definition erarbeitet. Unter Zuhilfenahme einer Expertenbefragung werden die acht wichtigsten Hinweise identifiziert, die Nutzer auf den Seiten eines Webshops verwenden können, um sich ein Bild über den jeweiligen Umgang mit personenbezogenen Daten zu machen. Um im Rahmen einer Blickbewegungsanalyse quantifizieren zu können, inwieweit diese Hinweise genutzt werden, wird die Messgröße der Fixation im Rahmen dieser Arbeit definiert.
Das entwickelte Studiendesign stellt die Grundlage für die Überprüfung eines Arbeitsmodells bezüglich potentieller Einflussgrößen auf tatsächliches Datenschutz-Verhalten beim Onlineshopping dar. Eine explorative Studie führt zu ersten Erkenntnissen bezüglich möglicher Prädiktoren. Für eine Validierung wird das Arbeitsmodell angepasst und eine Validierungsstudie durchgeführt, deren Design dem der Explorationsstudie entspricht.
Die Analyse der Blickbewegungen im Rahmen beider Studien zeigt, dass alle Hinweise insgesamt wenig zur Orientierung verwendet werden. Am häufigsten wird der Hinweis *Shopname (URL)* fixiert (23 von 73 Teilnehmern). Der höchste Wert für tatsächliches Datenschutz-Verhalten beim Onlineshopping, der sich aus der Summe der betrachteten wichtigsten Hinweise errechnet, beträgt nur vier der acht möglichen.
Das Alter der Teilnehmer kann als signifikanter Prädiktor nachgewiesen werden, der allerdings nur zu einem geringen Anteil an Varianzaufklärung führt. Der, auch im Rahmen dieser Studien nicht signifikante, Zusammenhang zwischen der erfragten Wahrscheinlichkeit für ein Verhalten und dem entsprechenden tatsächlichen Verhalten steht im Einklang mit den Erkenntnissen zum Privacy Paradoxon. Das beweist, dass die Intention im Rahmen von Datenschutz keinen akkuraten Prädiktor für tatsächliches Verhalten darstellt und bekräftigt die Notwendigkeit der empirischen Erfassung von tatsächlichem Verhalten für weitere Forschung in diesem Kontext. Das im Rahmen dieser Arbeit entstandene Untersuchungskonzept kann dem einen Rahmen geben und unmittelbar für weitere Untersuchungen verwendet werden, die das tatsächliche Datenschutz-Verhalten beim Onlineshopping als Variable beinhalten.

Abbildungsverzeichnis

Abbildung 1. Modell der Theorie des überlegten Handelns (Fishbein & Ajzen, 1975). *21*
Abbildung 2. Darstellung der Theorie des geplanten Verhaltens (Ajzen, 1985, nach eigener Darstellung). *22*
Abbildung 3. Modell der Protection Motivation Theory von Rogers (1975). *23*
Abbildung 4. Modell zur Vorhersage des Öffnens eines Emailanhanges von Pfeiffer et al. (2013). *28*
Abbildung 5. Darstellung der visuellen Informationsaufnahme und der Reizweiterleitung aus Goldstein (2008, S. 30). *39*
Abbildung 6. Darstellung der in der Literatur gefundenen Definitionen für Fixationen, mit Hilfe eines Zeitstrahls. *54*
Abbildung 7. Regler im Rahmen der visuellen Analogskala bezüglich der Einschätzung der Wichtigkeit der Hinweise mittels eines kurzen Blickes (Symbol Auge) bzw. einer eingehenderen Beschäftigung (Symbol Leselupe). *55*
Abbildung 8. Aus, in Kapitel 2.4.1 dargestellten Erkenntnissen abgeleitetes Arbeitsmodell zur Vorhersage tatsächlichen Verhaltens. *68*
Abbildung 9. Versuchsaufbau aus Sicht der Versuchsleiterin (aus Magin, 2013). *71*
Abbildung 10. Versuchsaufbau aus Sicht der Teilnehmer (aus Magin, 2013). *72*
Abbildung 11. Verteilung der errechneten Gesamtanzahl internetfähiger Geräte. *80*
Abbildung 12. Screenshot einer Webseite mit den entsprechenden Areas of Interests (AOI). *85*
Abbildung 13. Verteilung des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping auf Basis der Ergebnisse der Explorationsstudie. *88*
Abbildung 14. Angepasstes Modell zur Vorhersage des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping. *95*
Abbildung 15. Modell zur Vorhersage der Handlung im Internet Daten anzugeben, ohne die Datenschutzerklärungen angeschaut zu haben, mit Hilfe des entsprechenden wahrgenommenen Risikos, des erwarteten Nutzens und der angegebenen Wahrscheinlichkeit. *95*
Abbildung 16. Aufbau im Rahmen der Validierungsstudie (aus Becker, 2015; Dörner, 2015). *96*
Abbildung 17. Angegebener höchster Bildungsabschluss der Probanden der Validierungsstudie. *100*
Abbildung 18. Angegebenes Haushaltsnettoeinkommen der Probanden der Validierungsstudie. *100*
Abbildung 19. Verteilung des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping auf Basis der Ergebnisse der Validierungsstudie. *103*
Abbildung 20. Validiertes Modell zur Vorhersage von Datenschutz-Verhalten beim Onlineshopping. *108*
Abbildung 21. Nachgewiesener Zusammenhang bezüglich des Modells zur Vorhersage des tatsächlichen Verhaltens im Internet Daten anzugeben, ohne vorher die Datenschutzerklärungen angeschaut zu haben. *108*

Tabellenverzeichnis

Tabelle 1. Identifizierte Arten von Risiko im Rahmen von Onlineshopping. 12
Tabelle 2. Angaben in der Literatur bezüglich der Beschreibung von Fixationen. 43
Tabelle 3. Hinweise zur Einschätzung der Vertrauenswürdigkeit eines Webshops. 51
Tabelle 4. Mittelwerte (x), Standardabweichung (s), Minimum (Min) und Maximum (Max) der Wichtigkeit der Überprüfung auf Vorhandensein (kurzer Blick) und der Wichtigkeit einer eingehenderen Betrachtung (langer Blick) für die Hinweise auf den Umgang mit personenbezogenen Daten auf einer Skala von „unwichtig" (0) bis „wichtig" (100). 57
Tabelle 5. Zusammenfassende Rangreihe der wichtigsten Hinweise auf den Umgang mit personenbezogenen Daten. 59
Tabelle 6. Mittelwerte (Skala von „unwichtig" (0) bis „wichtig" (100)) der acht wichtigsten Hinweise nach dem Ranking im Rahmen der Gewichtungsstudie. 60
Tabelle 7. Ergebnisse des Shapiro-Wilk Tests auf Normalverteilung (p-Werte) der Variablen der eingeschätzten Wichtigkeit für eine kurze Überprüfung auf Vorhandensein des entsprechenden Hinweises. 61
Tabelle 8. Ergebnisse des Shapiro-Wilk Tests auf Normalverteilung (p-Werte) der Variablen der eingeschätzten Wichtigkeit für eine eingehendere Betrachtung des entsprechenden Hinweises. 62
Tabelle 9. Ergebnis des t-tests für abhängige Stichproben. 63
Tabelle 10. Hypothesen bezüglich der Variable Alter. 69
Tabelle 11. Versuchsablauf. 73
Tabelle 12. Gesamte deskriptive Ergebnisse der Explorationsstudie. 77
Tabelle 13. Deskriptive Ergebnisse der Explorationsstudie bezogen auf die für die Blickbewegungsanalyse herangezogenen Teilnehmer. 82
Tabelle 14. Blickbewegungsdaten der Explorationsstudie bezüglich der Hinweise auf die Vertrauenswürdigkeit eines Webshops (Vpn = Anzahl der Versuchspersonen, Fix. = Fixationen, NDwell Time = Normalized Dwell Time). 87
Tabelle 15. Ergebnisse der sign. Mann-Whitney-U-Tests und eines t-Test (inklusive der Gruppeneinteilung und der entsprechenden Mittelwerte (MW)), die zum Verwerfen der entsprechenden Nullhypothesen geführt haben. 89
Tabelle 16. Deskriptive Ergebnisse der Validierungsstudie. 97
Tabelle 17. Ergebnisse der Validierungsstudie bezüglich der Blickbewegungsanalyse hinsichtlich der wichtigsten acht Hinweise und der Hinweise Preis, Produktbeschreibung und Produktbild 102
Tabelle 18. Deskriptive Daten der aggregierten Stichprobe. 103
Tabelle 19. Zusammenfassung der Ergebnisse der Blickbewegungsanalysen bezüglich der acht wichtigsten Hinweise. 104

Inhaltsverzeichnis

1 Einleitung *1*

1.1 Motivation **1**
1.2 Zielsetzung der Arbeit **4**
1.3 Gliederung der Arbeit **4**

2 Stand der Forschung und Technik *6*

2.1 Definitionen **6**
2.1.1 Datenschutz und Datensicherheit 6
2.1.2 Verhalten vs. Handlung 7
2.1.3 Onlineshopping 8
2.1.4 Datenschutz-Verhalten beim Onlineshopping 8
2.1.5 Risiko 8
2.1.6 Signal und Hinweis 9
2.1.7 Wissen 10

2.2 Risiken beim Onlineshopping **10**
2.2.1 Risiko bezüglich der personenbezogenen Daten im Rahmen von Onlineshopping 13
2.2.2 Wahrscheinlichkeit für Angriffe auf personenbezogene Daten im Rahmen von Onlineshopping 14
2.2.3 Potentielle Konsequenzen von Angriffen auf personenbezogene Daten 15

2.3 Sicherung des Datenschutzes **16**
2.3.1 Absicherung durch den Staat 16
2.3.2 Technische Möglichkeiten der Absicherung 17
2.3.3 Sicheres Verhalten 18

2.4 Menschliches Verhalten im Kontext von Risiko **19**
2.4.1 Einflussfaktoren auf menschliches Verhalten im Kontext von Risiko 20
2.4.2 Umgang mit Risiken im Kontext des Internets 29
2.4.3 Studien zur Erfassung von Risikoverhalten 31

2.5 Erfassung von Verhalten mittels Blickbewegungsanalyse **37**
2.5.1 Geschichte der Blickbewegungsanalyse 37
2.5.2 Bilderfassung 39
2.5.3 Bildanalyse 41
2.5.4 Blickbewertung 45
2.5.5 Vor- und Nachteile des Verfahrens 45

2.6 Zusammenfassung und Forschungsfragen **46**

3 Vorgehen zur empirischen Erfassung von Datenschutz-Verhalten beim Onlineshopping *49*

3.1 Operationalisierung von tatsächlichem Datenschutz-Verhalten **49**
3.1.1 Hinweise zur Einschätzung der Vertrauenswürdigkeit eines Webshops 50
3.1.2 Konkretisierung der Blickbewegungsanalyse 52

3.2 Quantifizierung der aufgezeichneten Daten **54**
3.2.1 Vorgehen Gewichtungsstudie 54

3.2.2 Ergebnisse Gewichtungsstudie 56
3.2.3 Diskussion Gewichtungsstudie 63

3.3 Anforderungen an die Erhebung 64

4 Ermittlung potentieller personenbezogenen Prädiktoren 67

4.1 Ableitung des Arbeitsmodells und Hypothesen 67
4.2 Explorationsstudie 70
4.2.1 Vorgehen Explorationsstudie 71
4.2.2 Verwendete Methoden 74

4.3 Ergebnisse Explorationsstudie 77
4.3.1 Ergebnisse bezüglich der demographischen Attribute 79
4.3.2 Ergebnisse bezüglich der Erfahrung 79
4.3.3 Ergebnisse bezüglich der Einschätzungen der Risikosituationen 81
4.3.4 Ergebnisse bezüglich der Aufgabe 81
4.3.5 Ergebnisse bezüglich der Blickbewegung 84
4.3.6 Ergebnisse bezüglich des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping 88

4.4 Ergebnisse bezüglich des Potentials der Prädiktoren 89
4.5 Diskussion der Explorationsstudie 91

5 Vorhersage von Datenschutz-Verhalten beim Onlineshopping 94

5.1 Anpassung des Arbeitsmodells 94
5.2 Vorgehen Validierungsstudie 95
5.2.1 Anpassungen der Studie 96

5.3 Ergebnisse Validierungsstudie 97
5.3.1 Ergebnisse bezüglich der demographischen Attribute 99
5.3.2 Ergebnisse bezüglich der Erfahrung 101
5.3.3 Ergebnisse bezüglich der Einschätzungen der Risikosituationen 101
5.3.4 Ergebnisse bezüglich der Blickbewegung 101
5.3.5 Ergebnisse bezüglich des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping 102

5.4 Ergebnisse bezüglich der Vorhersage von Datenschutz-Verhalten 103
5.5 Validierte Modelle des Datenschutzverhaltens beim Onlineshopping 108

6 Diskussion 109

6.1 Diskussion bezüglich der verwendeten Methoden 111
6.1.1 Expertenbefragung via Online-Fragebogen 112
6.1.2 Fragebögen der Explorations- und Validierungsstudie 112
6.1.3 Online-Aufgabe und Interview 113
6.1.4 Blickbewegungsanalyse 114

6.2 Diskussion des Studiendesigns der Explorations- und Validierungsstudie 116
6.3 Diskussion der Stichproben im Rahmen der Explorations- und der Validierungsstudien 117

7 Fazit und Ausblick 119
Literaturverzeichnis 122
Anhangsverzeichnis 136

1 Einleitung

1.1 Motivation

Bis zum heutigen Tag steigt die Zahl derer, die das weltweite dezentralisierte Netzwerk (Amichai-Hamburger & Vinitzky, 2010) des Internets nutzen (Initiative D21, 2018). Eine Umfrage im Rahmen der Initiative D21 mit 20 424 Befragten ab 14 Jahren ergab, dass der Nutzeranteil der deutschen Bevölkerung im Jahr 2017 bei 81% lag (2018). Von diesen nutzten 96% das Internet im selben Jahr, um online Produkte zu erwerben (Bitkom, 2017b). Im Jahr 2017 wurde jeder zehnte Euro der Deutschen im Internet ausgegeben (Frankenpost Verlag GmbH, 2018). Allein im Warenhandel in Deutschland führte dies zu einem Umsatz von 58.47 Milliarden Euro (Berufsverband E-Commerce und Versandhandel Deutschland, 2018), Tendenz steigend (HDE Handelsverband Deutschland, 2018). Doch nicht nur das Geld der Nutzer ist ein begehrtes Gut des Internets. Schon 2012 nannte Sarah Spiekermann von der Wirtschaftsuniversität Wien personenbezogene Daten das „Öl der Informationsgesellschaft und eine eigene Vermögensklasse“ (heise online, 2012). Ein Beispiel hierfür ist die Tatsache, dass Unternehmen wie Google oder Facebook, die auf datenbasierten Geschäftsmodellen aufbauen (Buxmann, 2015), weltweit im Jahr 2016 zu den fünf umsatzstärksten Internetunternehmen gehörten (Kleiner Perkins Caufield & Byers, CB Insights, Wall Street Journal & S&P Capital IQ, 2017). Aber auch klassische Unternehmen nutzen mittlerweile Kundendaten, um das Verhältnis zu intensivieren und individuellere Produkte und Services anbieten zu können (Buxmann, 2015). Eine Nutzungsmöglichkeit persönlicher Kundendaten stellt die sogenannte personalisierte Werbung dar (Wambach, 2017). Hierbei werden die von dem jeweiligen Nutzer gesammelten Daten, z. B. bezüglich gesuchter Produkte, dazu genutzt für ihn passende Werbung einzublenden. Für den Nutzer[1] kann das ein Vorteil sein. So reduziert sich dadurch für ihn die irrelevante Werbung und die Zeit, passende Produkte zu finden (McDonald & Cranor, 2010). Mittels exakter Standortbestimmung ist es darüber hinaus möglich, ein interaktives Einkaufserlebnis zu generieren (Buxmann, 2015).

Neben der oft legalen Verwendung der Daten z. B. für personalisierte Werbung spielt der sogenannte Identitätsdiebstahl eine immer größere Rolle. Laut Bundeskriminalamt (2018) umfasst die digitale Identität „alle Arten von Accounts und zahlungsrelevanten Informationen eines Internetnutzers“. Laut dem Bundeslagebild Cybercrime 2017 des Bundeskriminalamtes ist es aufgrund der Gegebenheiten der statistischen Schadenserfassung nicht möglich, belastbare Aussagen über den, speziell durch Identitätsdiebstahl, bzw. –missbrauch hervorgerufenen monetären Schaden zu machen. Darüber hinaus ist es schwierig bis unmöglich, Schäden wie Reputationsverlust oder ein zeitweise außer Funktion gesetztes Netzwerk zu beziffern (Bundeskriminalamt, 2017).

Die Gefahr eines Missbrauchs ihrer Daten sorgt die Nutzer (Buxmann, 2015). Laut Miyazaki und Fernandez (2001) wird der Anstieg der Internetnutzung begleitet von Sorgen bezüglich Datenschutz und Datensicherheit. Park & Kim erwähnen schon 2003 die Sorge der Nutzer darüber, ihre privaten und finanziellen Informationen preiszugeben. Eine Analyse des Institutes für Demoskopie in Allensbach zeigte allerdings, dass sich diese Sorgen scheinbar nicht im Verhalten der Nutzer abzeichnen (Köcher, 2015). Obwohl sich die Nutzer sorgen, nutzen sie Dienste wie Onlinebanking oder Onlineshopping (Köcher, 2015). Dasselbe zeigten Umfragen bezüglich Diensten wie Facebook und Google (Buxmann, 2015). Täglich werden Computerbenutzer mit scheinbar unbedeutenden Sicherheitsentscheidungen konfrontiert (Hardee, Mayhorn & West, 2016). Acquisti und Grossklags (2005) kamen zu dem Schluss,

[1] Es sind stets Personen männlichen und weiblichen Geschlechts gleichermaßen gemeint; aus Gründen der einfacheren Lesbarkeit wird im Folgenden meist nur die männliche Form verwendet.

dass Menschen bereit sind, den Schutz ihrer Daten zugunsten Bequemlichkeit oder gegen relativ kleine Belohnungen einzutauschen. Zusätzlich seien sie selten bereit, Technologien zum Schutz der Privatsphäre zu verwenden. Auch Norberg, Horne und Horne (2007) waren in der Lage dieses Phänomen, welches sie das *privacy paradox* nennen, nachzuweisen. Sie meinen damit, dass Menschen bezüglich des Schutzes ihrer Daten nicht das tun, was sie sagen. Im Gegensatz zu den oben genannten Studien schafften Norberg et al. (2007) es dabei, tatsächliches Verhalten zu erfassen und nicht indirekt abzufragen. Denn hier liegt ein Problem dieses Forschungsgebietes. In den meisten Fällen wird das Verhalten, welches Nutzer zum Schutz ihrer Daten zeigen oder eben nicht zeigen, nur hypothetisch erfasst, was zu einer begrenzten Übertragbarkeit der Ergebnisse führt (Buxmann, 2015). Die Schwierigkeit besteht darin, das tatsächliche Verhalten von Menschen möglichst ohne deren Beeinflussung zu messen. Das, was gemessen wird, ist häufig die Bereitschaft, der Wille oder die Intention ein bestimmtes Verhalten zu zeigen (Norberg et al., 2007), nicht das Verhalten selbst. Im Falle von Datenschutz scheint die Intention allerdings kein akkurater Prädiktor für tatsächliches Verhalten zu sein (Norberg et al., 2007). Auch andere Themenbereiche stehen vor dieser Schwierigkeit. Im Bereich der Technologienutzung ist hier von der sogenannten *Intention-Behavior Gap* die Rede (Bhattacherjee & Sanford, 2009). Im Kontext der Risiko-Forschung existiert darüber hinaus aber die Besonderheit, dass Menschen, deren Verhalten man in einer solchen Risikosituation erfassen möchte, aufgrund von ethischen Gesichtspunkten nicht in eine Situation gebracht werden dürfen, in der sie einem tatsächlichen Risiko ausgesetzt sind (Döring & Bortz, 2016).

Um Aussagen über die Risikobereitschaft oder das Risikoverhalten von Personen machen zu können, wird diese deshalb oft im Rahmen von Aktivitäten erhoben, bei denen sich ein Risiko für die jeweilige Person in vertretbaren Grenzen hält. Geht man davon aus, dass die Persönlichkeit eines Menschen sich auf einer Skala von risikoavers bis risikosuchend einordnen lässt (Weber, Blais & Betz, 2002), so ließen sich die so gewonnenen Ergebnisse auf andere Situationen übertragen. Stattdessen wurde aber mehrfach bewiesen, dass sich die Risikobereitschaft, bzw. die Einstellung gegenüber einem Risiko abhängig vom jeweiligen Kontext und der jeweiligen Situation unterscheidet (z. B. Schoemaker, 1990; Weber et al., 2002). Um Aussagen über Verhalten in einem bestimmten Kontext machen zu können, muss das Verhalten in eben dem Kontext untersucht werden. Aus diesem Grund unterscheiden sich durchgeführte Studien in diesem Rahmen sehr.

Byrnes, Miller und Schafer (1999) führten eine Meta-Analyse über 150 Studien zum Eingehen von Risiken durch. Sie bezogen dabei allerdings nur die Studien ein, die in dem Zusammenhang Unterschiede zwischen den Geschlechtern untersuchten. Diese teilten sie zunächst in drei Kategorien, abhängig von der verwendeten Aufgabe ein. Im nächsten Schritt wurden auf Basis des Inhalts innerhalb der drei Kategorien bis zu acht weitere Untergruppen gebildet. Dies soll aufzeigen, wie breit das Thema aufgestellt ist.

Keine, der in der Metaanalyse einbezogenen Studien, befasst sich mit dem Thema Risiko in Bezug auf die persönlichen Daten. In der Zeit nach 1999 änderte sich dies. Einige der wenigen, in deren Rahmen tatsächliches Verhalten erfasst und nicht erfragt wurde, sind in Kapitel 2.4.3 vorgestellt. Hier werden auch die von den jeweiligen Wissenschaftlern genannten Einschränkungen aufgeführt, denen diese Studien unterliegen. So schützten z. B. Whalen und Inkpen (2005) oder auch Wu, Miller und Garfinkel (2006) ihre Probanden, indem sie ihnen unechte Daten (Fake-Accounts) zu Verfügung stellten. Schechter, Dhamija, Ozment und Fischer (2007) konnten in ihrer Studie nachweisen, dass Probanden, die somit nur eine Rolle spielten, ihre Daten weniger schützten als Probanden, die ihre eigenen Daten einsetzten. Darüber hinaus schränkten sowohl Whalen und Inkpen (2005) als auch Schechter et al. (2007) ein, dass die Untersuchung im universitären Umfeld durchgeführt wurde. Die Tatsache, dass in diesem Rahmen eine Einverständniserklärung unterschrieben wurde, die den Schutz der persönlichen

Daten verspricht, führt vermutlich zusätzlich dazu, dass die Teilnehmer zumindest ein geringeres Risiko wahrnehmen. Es wird darüber hinaus vermutet, dass eine Aufwandsentschädigung für die Teilnahme den Fokus entgegen eventueller Bedenken bezüglich einem Risiko, mehr auf die Aufgabenerfüllung legt (Schechter et al., 2007). Hiervon gehen Egelman, Cranor und Hong (2008) auch unabhängig von einer Entlohnung im Rahmen einer Laborstudie aus. Tsai, Egelman, Cranor und Acquisti (2011) merken an, dass die Probanden in ihrer Studie eventuell kein reales Verhalten zeigten, da ihnen die Produkte, die sie im Rahmen des Versuchs kaufen sollten, vorgegeben wurden. Beresford, Kübler und Preibusch (2012) schränkten dagegen die Auswahl der zu Verfügung stehenden Webshops auf zwei (unechte) ein. Eine Auswahl zwischen nur zwei Alternativen entspricht jedoch selten einer realen Einkaufssituation (Helmert, Symmank, Pannasch & Rohm, 2017).

Sollte es gelungen sein, das tatsächliche Verhalten in einer Risikosituation zu erfassen, ergibt sich eine weitere Schwierigkeit, nämlich die der Übersetzung des beobachteten Verhaltens in Zahlen, die für statistische Analysen verwendet werden können. In der Wissenschaft wird diese Übersetzung Operationalisierung genannt (z. B. Döring & Bortz, 2016; Huber, 2005). Laut Döring und Bortz (2016) sollte hierbei folgendermaßen vorgegangen werden: Im ersten Schritt ist es notwendig, alle relevanten Merkmale bezüglich aufgestellter Hypothesen zu definieren. Danach sollte eine Auswahl geeigneter Indikatoren und Datenerhebungsinstrumenten stattfinden, die es ermöglichen, die Konzepte zu messen. Huber (2005) erwähnt diesbezüglich, dass die Suche nach geeigneten Indikatoren für eine gute Operationalisierung sorgfältig vonstattengehen muss, da eine schlechte Operationalisierung die Testung von Hypothesen nutzlos macht. Im Rahmen der eigentlichen Messung werden dem beobachteten Verhalten Zahlenwerte (sogenannte Skalenwerte) zugeordnet, deren Relationen empirische Relationen repräsentieren (Huber, 2005). In diesem konkreten Fall bedeutet das, dass der Skalenwert einer Person, die ein ausgeprägtes Datenschutz-Verhalten zeigt, höher sein muss, als der Skalenwert einer Person, die keinerlei Maßnahmen ergreift, um die persönlichen Daten zu schützen. Abhängig von der jeweiligen Operationalisierung ergibt sich das Skalenniveau der Variablen, welches dann wiederum die Möglichkeiten der statistischen Auswertung bestimmt (Döring & Bortz, 2016). Für die Studie bedeutsame Variablen sollten möglichst valide gemessen und auf einem hohen Skalenniveau vorliegen (Döring & Bortz, 2016).

Konnten unter Beachtung dessen, allen Teilnehmern einer Studie repräsentative Werte zugeordnet werden, dann ist es, je nach Skalenniveau, möglich, zugrundeliegende Einflussfaktoren auf das Verhalten aufzudecken und deren Einfluss zu untersuchen. Die Motivation dafür könnte darin liegen, dass unpassendes/-schönes/-gesundes Verhalten verändert werden soll. Das Kennen des jeweiligen Verhaltens stellt hierfür die Grundlage dar. So ist eine Intervention anders erfolgreich, wenn risikoreiches Verhalten auf einer unrealistischen Einschätzung des Risikos beruht, als wenn das Verhalten sich auf einem pathologischen Hang zum Risiko begründet (Weber et al., 2002). Auch Page und Uncles (2004) erwähnen, dass das Wissen über Kenntnisse und Verhalten der Nutzer es ermöglicht, diese mittels geeigneter Technologien zu unterstützen. Denn das Wissen über Prozesse, die dem Verhalten zugrunde liegen, ist notwendig für eine nützliche Intervention (Downs, Holbrook & Cranor, 2006; Weber et al., 2002).

Im Kontext des Themas Datenschutz ist zusätzlich zu erwähnen, dass einzelne Nutzer abhängig von ihrem Verhalten nicht ausschließlich ihre eigenen Daten in Gefahr bringen (Anderson & Agarwal, 2010), sondern z. B. im Umgang mit sozialen Medien, Einfluss auf die Sicherheit der Daten von anderen, bis hin zu Unternehmensdaten haben. Da private Nutzer im Gegensatz zur Arbeitsumgebung nicht durch Training oder Fachleute dabei unterstützt werden z. B. Sicherheitssoft und -hardware aktuell zu halten, stellen diese laut Anderson und Agarwal (2010) das „schwächste Glied in der Kette“ dar. Sie bemängeln darüber hinaus, dass ein mangelndes Verständnis darüber existiert, was die Nutzer dazu bringt, sich

sicher zu verhalten, bzw., wie man das Verhalten beeinflussen kann. Genau dieses Wissen ist aber notwendig, um Produkte zu entwickeln, die Nutzer unterstützen können (Downs et al., 2006). Laut Hargittai (2007) werden in vielen Studien zu wenige Charakteristika der Nutzer erhoben, was es unmöglich macht unterschiedliches gezeigtes Verhalten damit in Verbindung zu bringen.

Fazit

Ungefähr 78% der deutschen Bevölkerung nutzten im Jahr 2017 die Möglichkeit des Onlineshoppings. Deren Daten stellen im Internet ein begehrtes Gut dar, welches die Nutzer schützen sollten. Danach befragt, geben sie auch überwiegend an, dies zu tun. Das entspricht aber häufig nicht ihrem Verhalten. Tatsächliches Verhalten in einer Risikosituation ist schwierig zu erfassen und sehr kontextspezifisch. Eine zusätzliche Schwierigkeit stellt die Übersetzung des beobachteten Verhaltens in repräsentative Daten dar. Eine erfolgreiche Überwindung der genannten Schwierigkeiten würde, zusammen mit der Erhebung entsprechender Charakteristika der Nutzer, zu Erkenntnissen bezüglich Einflussfaktoren auf das entsprechende Verhalten führen. Aus diesen ließen sich im Folgenden Gestaltungshinweise z. B. für eventuelle Unterstützungssysteme ableiten.

1.2 Zielsetzung der Arbeit

Ein Ziel dieser Arbeit in Bezugnahme auf das vorangegangene Kapitel ist, die Entwicklung eines Studiendesigns zur empirischen Erfassung möglichst realistischen Verhaltens zum Schutz der eigenen Daten im Rahmen von Onlineshopping. Hierfür muss im ersten Schritt eine geeignete Operationalisierung des Verhaltens erarbeitet werden. Zusätzlich muss eine Möglichkeit gefunden werden das erfasste Verhalten in aussagekräftige Daten zu übersetzen, die für spätere Analysen geeignet sind. Die Identifikation von Prädiktoren auf das Verhalten und dessen Vorhersage stellen weitere Ziele der Arbeit dar. Da personenbezogene Einflussfaktoren zu situationsunabhängigen Vorhersagen führen, stellen sie eine gute Grundlage für Interventionen und Unterstützungen dar. Aus diesem Grund sollen ausschließlich Größen untersucht werden, die sich auf die Person der Nutzer beziehen. Die Nutzung der Erkenntnisse zur Ableitung von Gestaltungshinweisen zur Entwicklung von Interventionen ist nicht Teil dieser Arbeit. Die Entwicklung eines umfassenden Modells zum Datenschutz-Verhalten ist ebenfalls kein angestrebtes Ziel.

1.3 Gliederung der Arbeit

Das erste Kapitel dieser Arbeit stellt die Motivation zur Entwicklung einer Methodik zur Erfassung von Datenschutz-Verhalten beim Onlineshopping vor (Kapitel 1.1). Die Ziele, die in diesem Rahmen gesteckt wurden, sind in Kapitel 1.2 beschrieben, gefolgt von der Beschreibung der Struktur, in der die Zielerreichung dargestellt wird (Kapitel 1.3). Das zweite Kapitel deckt inhaltlich den Stand der Forschung und Technik bezüglich der relevanten Inhalte ab. Zum besseren Verständnis werden zunächst notwendige Begriffe dargestellt und, wenn notwendig, abgegrenzt (Kapitel 2.1). Das nächste Kapitel (2.2) nimmt Bezug auf das Thema des Onlineshoppings als risikoreiche Handlung. Angepasst an die Definition von Risiko gliedern sich die folgenden Unterkapitel. Im Zuge dessen werden zunächst die Risiken, die sich in diesem Rahmen generell und speziell in Bezug auf den Schutz der persönlichen Daten ergeben, zusammengefasst (Kapitel 2.2.1). In Kapitel 2.2.2 wird dann der Versuch gemacht, eine Aussage über die Wahrscheinlichkeit des Verlustes der Daten zu machen. Mögliche Konsequenzen, die sich aus dem Diebstahl personenbezogener Daten ergeben können, sind Inhalt von Kapitel 2.2.3.

Möglichkeiten zur Abwendung der im vorigen Kapitel dargestellten Risiken werden unter Kapitel 2.3 beschrieben. Diese werden in staatliche Absicherungen (Kapitel 2.3.1), technische Möglichkeiten (Kapitel 2.3.2) und sicheres Nutzerverhalten (Kapitel 2.3.3) unterteilt. Kapitel 2.4 befasst sich mit Risikoverhalten. Dafür werden zunächst Modelle und Theorien zum Risikoverhalten vorgestellt und die Einflussfaktoren genannt (Kapitel 2.4.1). Kapitel 2.4.2 stellt dar, wie Nutzer mit den vorherrschenden Risiken im Internet umgehen. Unterschiedliche Möglichkeiten zur Erfassung von tatsächlichem Risikoverhalten in Bezug auf das Internet sind Inhalt von Kapitel 2.4.3. Die dort verwendeten Messgrößen für Risikoverhalten werden in Kapitel 2.4.3.1 zusammengefasst und die besondere Eignung der Blickbewegungsanalyse als Messmethode begründet. Die Erfassung von Verhalten mit der Blickbewegungsanalyse ist Inhalt von Kapitel 2.5. Hier wird neben der Darstellung der historischen Entwicklung der Blickbewegungsanalyse in Kapitel 2.5.1 auf die Komponenten Bilderfassung (Kapitel 2.5.2), Bildanalyse (Kapitel 2.5.3) und Blickbewertung (Kapitel 2.5.4) eingegangen. Den Abschluss hierzu bilden Vor- und Nachteile der Methode in Kapitel 2.5.5. Die Erkenntnisse aus Kapitel 2 werden unter Kapitel 2.6 zusammengefasst und mit den Zielen der Arbeit in Zusammenhang gebracht. Im Weiteren werden aus den dargestellten Forschungslücken entsprechende Forschungsfragen abgeleitet. Die Bearbeitung von *Forschungsfrage 1* ist in Kapitel 3 dargestellt. Hierfür wird zunächst eine Operationalisierung von tatsächlichem Datenschutz-Verhalten beim Onlineshopping erarbeitet. Dafür wird im ersten Schritt eine Liste von Hinweisen zur Einschätzung der Vertrauenswürdigkeit eines Webshops erstellt (Kapitel 3.1.1) und dann die notwendigen Messgrößen bezüglich der Blickbewegungsanalyse konkretisiert (Kapitel 3.1.2). Im Rahmen von Kapitel 3.2 wird die Übersetzung potentiell beobachteten Verhaltens in Zahlenwerte vorbereitet. Dafür wurde eine Gewichtungsstudie in Form einer Expertenbefragung durchgeführt, deren Vorgehen (Kapitel 3.2.1) und Ergebnisse (Kapitel 3.2.2) dargestellt und in Kapitel 3.2.3 diskutiert werden. Den Abschluss des Kapitels bildet die Ableitung von Anforderungen, die sich an eine Studie stellen, mit Hilfe derer die erarbeitete Operationalisierung erfasst werden kann. Die sich ergebende Explorationsstudie ist in Kapitel 4 dargestellt. Hierfür wird zunächst ein Arbeitsmodell abgeleitet (Kapitel 4.1), welches die Grundlage der Studie (Kapitel 4.2) bildet. Deren Vorgehen (Kapitel 4.2.1) und die verwendeten Methoden (Kapitel 4.2.2) werden beschrieben, bevor die erhaltenen Ergebnisse in Kapitel 4.3 und 4.4 dargestellt werden. Die Diskussion der Explorationsstudie (Kapitel 4.5) schließt das Kapitel. Mit der Vorhersage von Datenschutz-Verhalten und somit mit der Beantwortung von *Forschungsfrage 2* und *Forschungsfrage 3* beschäftigt sich Kapitel 5. Hierfür wird in einem ersten Schritt das bestehende Arbeitsmodell auf Basis der Erkenntnisse aus der Explorationsstudie angepasst (Kapitel 5.2.1). Das Vorgehen der folgenden Validierungsstudie (Kapitel 5.2) und insbesondere die Anpassungen in Bezug auf die Explorationsstudie (Kapitel 5.2.1) werden dargestellt. Die erhaltenen Ergebnisse (Kapitel 5.3 und 5.4) und die sich ergebenden validierten Modelle (Kapitel 5.5) führen zur Beantwortung der beiden Forschungsfragen. Kapitel 6 beinhaltet eine ausführliche Diskussion des gesamten Vorgehens, der verwendeten Methoden (Kapitel 6.1), des im Rahmen der Explorations- und der Validierungsstudie verwendeten Studiendesigns (Kapitel 6.2) und der erhaltenen Stichprobe (Kapitel 6.3). Kapitel 7 schließt die Arbeit mit einem Fazit und Ausblick auf die Möglichkeit weiterer Untersuchungen im Kontext dieser Arbeit ab.

2 Stand der Forschung und Technik

Im Rahmen dieses Kapitels wird der aktuelle Stand zu Forschung und Technik bezüglich Datenschutz-Verhalten beim Onlineshopping beleuchtet. Dafür werden in Kapitel 2.1 zunächst grundlegende Begriffe definiert. Vorhandene Risiken, denen sich Nutzer im Internet (2.2) und speziell beim Onlineshopping gegenübersehen (2.2.1), sowie deren Eintrittswahrscheinlichkeit (2.2.2) und sich ergebende Konsequenzen (2.2.3) sind Thema von Kapitel 2.2. Dem werden in Kapitel 2.3 unterschiedliche Arten der Absicherung gegenübergestellt. So sichert der Staat seine Bürger durch verschiedene Richtlinien und Gesetze ab (2.3.1). Darüber hinaus gibt es unterschiedliche technische Lösung um sich im Rahmen von Onlineshopping abzusichern (2.3.2). Abschließend werden Hinweise auf sicheres Verhalten beim Onlineshopping gegeben (2.3.3). Kapitel 2.4 befasst sich mit Verhalten von Menschen in Risikosituationen, indem zunächst kontextübergreifende und spezifischere Theorien und Modelle dargestellt werden (2.4.1). Die Tatsache, dass das, was Menschen in Studien sagen nicht unbedingt das ist, was sie auch tun, wird näher erläutert (2.4.2), bevor unterschiedliche Methoden der Erfassung von Risikoverhalten im Rahmen von Studien vorgestellt werden (2.4.3). Aus den dort verwendeten Methoden und Messgrößen wird die besondere Eignung der Blickbewegungsanalyse in diesem Kontext herausgearbeitet. Die Methode wird in Kapitel 2.5 gegliedert in historische Einführung (2.5.1), Bilderfassung (2.5.2), -analyse (2.5.3) und -bewertung (2.5.4) dargestellt. Eine Zusammenfassung der Erkenntnisse der vorangegangenen Kapitel und die Vorstellung der untersuchten Forschungsfragen in Kapitel 2.6 schließt den aktuellen Stand der Forschung und Technik ab.

2.1 Definitionen

Um einen übereinstimmenden Überblick über das gesamte Thema erlangen zu können, ist es notwendig einige der grundlegenden Begriffe, die in diesem Rahmen verwendet werden, genauer zu beleuchten und zu definieren.

2.1.1 Datenschutz und Datensicherheit

Die Bedeutung des Begriffes Datenschutz hat im Laufe der Jahre einen Wandel erfahren. So definierte zum Beispiel Pommerening (1991) in seinem Buch *Datenschutz und Datensicherheit* den Datenschutz noch als den „Schutz der Daten vor Missbrauch, unberechtigter Einsicht oder Verwendung, Änderung oder Verfälschung, aus welchen Motiven auch immer. Im engeren Sinne, etwa in der Gesetzgebung, handelt es sich dabei nur um personenbezogene Daten; im allgemeinen Sprachgebrauch, und so auch hier, werden aber alle Daten, die irgendwo gespeichert sind, einbezogen.“ (S.10). Als Datensicherheit beschreibt er den „angestrebte[n] Zustand, der durch alle […] Maßnahmen erreicht werden soll, aber letztlich nicht vollkommen erreicht werden kann.“ (S.10).
Auf seiner Webseite (klauspommerening.de, 2004) widerruft er dies und ruft dazu auf, den Begriff des Datenschutzes ausschließlich im juristischen Sinne zu verwenden. Juristisch hat der Datenschutz als „Recht auf informationelle Selbstbestimmung“, so wie er heute verstanden wird, seinen Ursprung im sogenannten Volkszählungsurteil (Boos, 2015) des Bundesverfassungsgerichts vom 15. Dezember 1983 (Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, o.D.) Weitere Informationen hierzu sind in Kapitel 2.3.1 zu finden.

Im Duden wird Datenschutz als der „Schutz des Bürgers vor Beeinträchtigungen seiner Privatsphäre durch unbefugte Erhebung, Speicherung und Weitergabe von Daten, die seine Person betreffen“ definiert (Duden, 2018b). Der Begriff *Daten* wird in dem Zusammenhang sowohl für „(durch Beobachtungen, Messungen, statistische Erhebungen u. a. gewonnene) [Zahlen]werte, (auf Beobachtungen, Messungen, statistischen Erhebungen u. a. beruhende) Angaben, formulierbare Befunde“, als auch für „elektronisch gespeicherte Zeichen, Angaben, Informationen“ verwendet (Duden, 2018a).
Anders als das Wort vermuten lässt, steht demnach nicht der Schutz der Daten, sondern der Schutz der Person im Fokus. Als „Sicherheit von Daten vor dem Zugriff Unbefugter“ ist dagegen der Begriff der Datensicherheit definiert (Duden, 2018c).
Es ist eine Sache der Auslegung, ob ein Nutzer, der seine Daten nicht angibt, damit seine Privatsphäre oder seine Daten schützt. Der Begriff der Datensicherheit umfasst dabei aber alle Arten von Daten, während diese im Rahmen des Datenschutzes auf personenbezogene Daten eingeschränkt sind. Da in dieser Arbeit der Aspekt des Schutzes der Privatsphäre der Nutzer im Vordergrund steht, wird im weiteren Verlauf der Begriff des Datenschutzes verwendet. Gemeint ist damit der Schutz der eigenen Person durch Schützen der privaten Daten.

2.1.2 Verhalten vs. Handlung

Da die Begriffe Verhalten und Handlung im Rahmen dieser Arbeit häufig verwendet werden, ist es notwendig, die dahinterstehende Unterscheidung darzustellen und sie als Phänomene wahrzunehmen. Laut Duden stellt das Handeln eine „bewusst ausgeführte Tat“ dar (Duden, 2018d), wohingegen Verhalten als die „Art und Weise, wie sich ein Lebewesen verhält“ definiert ist (Duden, 2018j). Mit *sich verhalten* ist dabei gemeint, „in bestimmter Weise auf jemanden, etwas in einer Situation o. Ä. reagieren“, bzw. „in seinem Handeln [anderen gegenüber] eine bestimmte Haltung, Einstellung zeigen; sich benehmen“ (Duden, 2018h). Ähnlich beschreibt auch Heckhausen (1989) den Unterschied zwischen Handlung und Verhalten. Er schließt sich dabei den Ausführungen von Max Weber (2002)(im Original 1921) an. Beide gehen dann von einer Handlung aus, wenn „der oder die Handelnden mit ihm einen subjektiven Sinn verbinden“ (Weber, 2002, S. 1). Die Verstehbarkeit und Nachvollziehbarkeit dieses Sinns durch Andere führe demnach dazu, dass die „Grenze sinnhaften Handelns gegen ein bloß […] reaktives, mit einem subjektiv gemeinten Sinn nicht verbundenes, Sichverhalten […] durchaus flüssig [sei]“ (Weber, 2002, S. 2). Aktivitäten, mit Hilfe derer das gleiche Ziel erreicht werden soll, können in ihrem Sinne als eine Handlung zusammengefasst werden (Heckhausen, 1989). Die nicht klar zu ziehende Grenze zwischen Handlung und Verhalten fasst Groeben (1986) in seiner Kategorie *Tun* zusammen. Er betrachtet Verhalten unter Aspekten wie Intentionalität, Willkürlichkeit, Planung und Sinnhaftigkeit und benennt den „Endpol des Kontinuums“ (S.169), welcher all das bedient mit *Handlung*. *Verhalten*, als der andere Endpol, bleiben seines Erachtens nur die „Phänomene“ übrig, „die überhaupt nicht mehr als intentionale (Handlungen) oder motivationale (Tuns-Einheiten) rekonstruierbar sind“ (Groeben, 1986, S. 404). Im Gegensatz zu einer solchen Gegenüberstellung beider Konzepte verwenden Badke-Schaub, Hofinger und Lauche (2008) Verhalten als Oberbegriff, „der u. a. die Tätigkeiten und Handlungen von Menschen einschließt“ (S.78). Unter Handlungen verstehen sie „relativ selbständige Abschnitte zielgerichteter Tätigkeiten, die Teilziele realisieren.“ (S.81). Damit entsprechen sie der Definition von Hacker, die in der *Enzyklopädie der Psychologie* zu finden ist (Hacker, 2010). Handlung wird darin als „die kleinste psychologisch relevante Einheit willentlich gesteuerter Tätigkeiten“ (S.7) definiert. Die im Rahmen dieser Arbeit verwendete Definition soll die von Martin Fishbein und Icek Ajzen sein. Bei ihnen handelt es sich um die Autoren der viel verwendeten Modelle

zur Vorhersage von Verhalten, der Theory of Reasoned Action (Fishbein & Ajzen, 1975) und der Theory of Planned Behavior (Ajzen, 1991). In ihrem gemeinsamen Buch zum aktuellen Stand ihrer Forschung (Fishbein & Ajzen, 2011) beschreiben sie Verhalten als beobachtbare Ereignisse, die sich aus vier Elementen zusammensetzen: die durchgeführte Handlung, das Ziel der Handlung, der Kontext, in welchem die Handlung steht, und die Zeit, in der die Handlung durchgeführt wurde. Über diese Elemente lässt sich ein Verhalten spezifizieren. Ändert sich ein Bestandteil, so handelt es sich laut den Autoren um ein anderes Verhalten. Dem ist die Überlegung geschuldet, wie spezifisch oder unspezifisch man die vier Elemente im Rahmen eines Versuchsaufbaus beschreibt, bzw. abfragt. Fishbein und Ajzen machen dies mit dem Hinweis deutlich, dass es wichtiger und auch interessanter ist zu erfahren, warum Menschen an Fitnesskursen teilnehmen und weniger, warum Menschen an genau einem speziellen Kurs teilnehmen. Mehrere Handlungen können zu einer Verhaltenskategorie aggregiert werden. Mit der Abfrage der Teilnahme an unterschiedlichen Fitnessangeboten (Handlungen) kann man sich demnach ein Bild bezüglich des Fitness-Verhaltens machen. Die Autoren geben darüber hinaus den Hinweis, dass der Einbezug von Ausmaß- oder Häufigkeitsmessungen zu Problemen bei der Erklärung von unterschiedlichem Verhalten führen kann. Sie empfehlen deshalb dichotome Kategorien zu verwenden.

2.1.3 Onlineshopping

Im Duden ist Onlineshopping als „Einkauf per Bestellung über das Internet“ definiert (Duden, 2018f). Dies entspricht der Definition des Gabler Wirtschaftslexikons, welches Onlineshopping als „wichtigen Teilbereich des E-Commerce“ nennt und als „Abwicklung von Kauftransaktionen (v. a. Konsum- und Gebrauchsgüter) mithilfe von Internettechnologien“ definiert (Lackes, Siepermann & Kollmann, 2018). Im Rahmen dieser Arbeit wird die etwas breitere Definition von Blake, Neuendorf und Valdiserri (2003) verwendet, die neben dem eigentlichen Kauf auch die Informationssammlung im Vorfeld eines Kaufs beinhaltet. So definieren Blake et al. (2003) Onlineshopping im Rahmen ihrer Studie als das Benutzen des Internets, um Informationen über Produkte, Dienstleistungen, Hersteller oder Firmen zu sammeln und/oder Produkte, Dienstleistungen usw. zu kaufen.

2.1.4 Datenschutz-Verhalten beim Onlineshopping

Schlussfolgernd aus Kapitel 2.1.1-2.1.3 wird *Datenschutz-Verhalten beim Onlineshopping* in dieser Arbeit definiert als eine Sammlung von Handlungen, die Nutzer im Kontext von Onlineshopping zeigen, die das Ziel haben die eigene Person und deren Privatsphäre zu schützen, indem die eigenen personenbezogenen Daten geschützt werden.

2.1.5 Risiko

Neben dem Begriff des Risikos werden in diesem Kapitel unterschiedliche Konstrukte dargestellt, die mit Risiko in Verbindung stehen, nämlich das wahrgenommene Risiko, die Risikobereitschaft und das Risikoverhalten. Global handelt es sich bei Risiko laut Duden um einen „mögliche[r]n negative[r]n Ausgang bei einer Unternehmung, mit dem Nachteile, Verlust, Schäden verbunden sind“, bzw. um ein „mit einem Vorhaben, Unternehmen o. Ä. verbundenes Wagnis“ (Duden, 2018g). In Bezug auf den Kauf von Produkten wird Risiko als die Möglichkeit eines zukünftigen Verlustes beschrieben, der den Wert

des Produktes zum Zeitpunkt des Kaufs, verringern kann (Sweeney, Soutar & Johnson, 1999). Laut Furby und Beyth-Marom (1992) handelt es sich dann um das Eingehen eines Risikos, wenn zwei Bedingungen erfüllt sind: Das fragliche Verhalten kann zu mehr als einem Ausgang führen und einige der Ausgänge sind unerwünscht oder sogar gefährlich. Das Ausmaß an Risiko wird häufig als das Produkt aus der potentiellen Schadenshöhe und der Eintrittswahrscheinlichkeit kalkuliert (Boos, 2015).
Sitkin und Pablo (1992) fassen zusammen, dass es sich bei Risiko um die Charakteristik einer Entscheidung handelt, bei der Unsicherheit bezüglich des möglichen Ausgangs besteht. Sie nennen zur Definition des Risikos drei Schlüsseldimensionen: die Unsicherheit bezüglich des Ausganges (*outcome uncertainty*), die Erwartungen bezüglich des Ausganges (*outcome expectations*) und das Potential/die Möglichkeit des Ausganges (*outcome potential*). Die drei Dimensionen können von unterschiedlichen Personen unterschiedlich eingeschätzt werden. Das Konstrukt, in dem sich die Personen dann unterscheiden, wird als wahrgenommenes Risiko betitelt. Dieses stellt laut Blais und Weber (2006) eine Funktion von Unsicherheit und der Aversion/Scheu (Aversiveness) gegenüber den Konsequenzen dar. So definieren Forsythe, Liu, Shannon und Gardner (2006) das wahrgenommene Risiko im Rahmen von Onlineshopping, als die subjektive Wahrnehmung des Nutzers bezüglich eines bestimmten Verlustes, der sich aus dem online Einkauf ergibt. Bei Biswas und Biswas (2004) stellt das wahrgenommene Risiko dagegen die Art und das Ausmaß an Unsicherheit dar, die ein Nutzer in einer bestimmten Kaufsituation empfindet.
Was für den einen Menschen eine Risikosituation darstellt, ist es für einen anderen eventuell nicht (Byrnes et al., 1999). Diese Annahme der Subjektivität impliziert laut Byrnes et al. (1999), dass Menschen nur dann ein Risiko eingehen, wenn sie sich dessen auch bewusst sind. Der Annahme widersprechen die Autoren mit dem Hinweis, dass es einige Beispiele für prototypische Risikoverhaltensweisen gibt, die aus Naivität gezeigt werden (z. B. ungeschützter Geschlechtsverkehr zwischen uninformierten Teenagern oder Kinder, die auf einer Straße spielen). Doch nicht nur interindividuell gibt es Unterschiede. Man geht heute von einer Interaktion zwischen der jeweiligen Person und der jeweiligen Situation aus, die das Verhalten bedingt (Blumer & Doering, 2012). So konnten z. B. Weber et al. (2002) unterschiedliche Risikodomains nachweisen (Vergleiche Kapitel 2.4.1). Bevor demnach Aussagen über stabile individuelle Unterschiede gemacht werden können, müssen situationelle Unterschiede kontrolliert oder eliminiert werden (Weber et al., 2002). Was dann relativ stabil bleibt, ist eine personenspezifische Bereitschaft, Nutzen und Risiko zu verrechnen, die sogenannte Risikoeinstellung (Blais & Weber, 2006; Weber & Hsee, 1998). Sie beschreibt die Form der individuellen Nutzenfunktion (Blais & Weber, 2006; Weber et al., 2002). Diese verläuft konkav bei risikoaversen/ risikoscheuen oder konvex bei risikofreudigen Entscheidern (Laux, 2005) (vergleiche Kapitel 2.4.1). Abhängig von Kontext bzw. Situation sind Menschen unterschiedlich bereit ein Risiko einzugehen. Die Bereitschaft, die auch Intention genannt wird, ist dabei von dem Risikoverhalten zu unterscheiden. Während es sich bei der Intention um die subjektiv wahrgenommene Wahrscheinlichkeit dafür handelt, dass ein bestimmtes (Risiko-) Verhalten gezeigt wird, ist das Verhalten das, was beobachtet werden kann (Fishbein & Ajzen, 2011).

2.1.6 Signal und Hinweis

Im Rahmen zweier Studien in dieser Arbeit werden Inhalte von Webseiten von Onlineshops verwendet, anhand derer sich Nutzer ein Bild von der Vertrauenswürdigkeit des Shops machen können. Ahrholdt (2010), verwendete dafür die Begriffe Schlüsselreize bzw. Signale. Andere Arbeiten, die mit ähnlichen Inhalten arbeiten, liegen in englischer Sprache vor. Hier werden die Worte „signals“ (Biswas & Biswas,

2004), „to signal“ (Bhattacherjee, 2014) oder „cues“ (Downs et al., 2006; Wang, Beatty & Foxx, 2004; Whalen & Inkpen, 2005) verwendet. Während die ersten beiden die Verwendung des Begriffes Signal nahelegen, wird „cues“ eher mit dem Begriff Hinweis übersetzt (Linguee Wörterbuch, 2018). Im Deutschen wird ein Signal u. a. als ein „optisches oder akustisches Zeichen mit einer bestimmten Bedeutung“ definiert (Duden, 2018i). Die Definition des Begriffes Hinweis lautet u. a. „Andeutung, hinweisende [An]zeichen für etwas“ (Duden, 2018e). Bei einigen, der im Rahmen dieser Arbeit verwendeten Inhalte der Webshops, entspricht ihre Bedeutung auch dem hier gegebenen Kontext. So fungiert ein Gütesiegel tatsächlich als Signal für eine Art Sicherheit oder ein https in der URL signalisiert eine verschlüsselte Verbindung. Andere untersuchte Inhalte stehen dafür vordergründig für etwas Anderes als Sicherheit. So haben die Angabe von Kontaktinformationen oder den Allgemeinen Geschäftsbedingungen in erster Linie rechtliche Gründe. Sie können Nutzern aber auch einen Hinweis auf die Vertrauenswürdigkeit bzw. die Sicherheit geben. Da der Begriff Hinweis die eigentliche Bedeutung des Inhaltes nicht einschränkt, soll dieser im Weiteren für die untersuchten Inhalte der Webseiten verwendet werden.

2.1.7 Wissen

Laut Duden stellt Wissen neben der Kenntnis von etwas, die „Gesamtheit der Kenntnisse [dar], die jemand (auf einem bestimmten Gebiet) hat“ (Duden, 2018k). Etwas ausführlicher wird das Wissen im Oxford dictionary (*knowledge*) als Fakten, Informationen und Fähigkeiten/Fertigkeiten beschrieben, die durch Erfahrung oder Erziehung erworben wurden (English Oxford Dictionaries, 2018). Speziell das Wissen in Bezug auf das Internet wird von Potosky (2007) zusammengefasst als das, was die Menschen über das Internet wissen und die vielen verschiedenen Dinge, die sie im Rahmen des Internets fähig sind zu tun. Dabei stellt das Wissen über den jeweiligen Kontext einen wichtigen Prädiktor in Bezug auf Verhalten dar (Pillai & Hofacker, 2007). Man unterscheidet dabei zwischen dem deklarativen und dem prozeduralen Wissen. Das deklarative Wissen ist definiert als sowohl Fakten- als auch komplexes Zusammenhangswissen, also das „Wissen, dass“ (Wild & Möller, 2009, S. 4). Das „Wissen, wie“ wird dagegen als prozedurales Wissen bezeichnet (Wild & Möller, 2009, S. 4). Laut Potosky (2007) ist es in Bezug auf Internet-Wissen wichtig, eine Kombination von Wissen über die Bedeutung verschiedener Begriffe und dem Wissen über spezifische Aufgaben-bezogene Handlungen zu erfassen, um das Konstrukt in adäquater Tiefe und Breite zu erfassen. In Bezug auf die Erfassung des Wissens unterscheidet man darüber hinaus zwischen dem objektiven Wissen und dem subjektiven Wissen. Das objektive Wissen stellt das absolute Wissen der Testperson dar und wird z. B. mittels objektiven Tests ermittelt (Alba & Hutchinson, 2000; Raju, Lonial & Mangold, 1995). Das, was die Person denkt, was sie weiß, wird als subjektives Wissen bezeichnet (Raju et al., 1995). Erhoben wird dieses Konstrukt mittels Selbstauskunft (Alba & Hutchinson, 2000; Raju et al., 1995). Dabei fällt auf, dass Menschen ihr objektives Wissen sehr häufig überschätzen (Alba & Hutchinson, 2000). Studien zu diesen Zusammenhängen ergaben überwiegend mittlere positive Korrelationen zwischen beiden Konstrukten (Raju et al., 1995). Eine Übersicht hierzu zeigen Carlson, Bearden & Hardesty (2007).

2.2 Risiken beim Onlineshopping

Viele Nutzer des Internets kaufen auch Produkte online. Dies bringt ihnen viele Vorteile. So sind Onlineshopping Nutzer weder an Öffnungszeiten gebunden, noch müssen sie zu Stoßzeiten überfüllte

Geschäfte aufsuchen (Boos, 2015). Darüber hinaus steht ihnen im Internet ein größeres Angebot, ein Mehr an Informationen und somit bessere Vergleichsmöglichkeiten zu Verfügung (Boos, 2015). Neben dem Schreiben und Erhalten von Emails und dem online Erledigen von Bankangelegenheiten gehört das Onlineshopping allerdings zu den Tätigkeiten im Internet, die ein gewisses Risiko und Unsicherheit beinhalten (Kim, Xu & Gupta, 2012).

Im Gegenteil zu herkömmlichen Ladengeschäften ist es im Internet schwer, zwischen seriösen und weniger seriösen Anbietern zu unterscheiden (Biswas & Biswas, 2004). Zusätzlich erschwert die erhebliche Anzahl die Auswahl eines geeigneten Anbieters (Biswas & Biswas, 2004). Unseriöse Anbieter haben es dabei leicht im Internet. So finden sie mit einer Webseite im Gegenteil zu einem Ladengeschäft günstig eine Plattform, um eventuell nicht einmal vorhandene Waren anzubieten (Boos, 2015). Dieser Umstand wird zusätzlich durch die physische und zeitliche Distanz zwischen Käufer und Verkäufer (Kim et al., 2012) begünstigt. Auch die Auswahl der Produkte ist teilweise dadurch erschwert, dass diese nicht in der Form überprüft werden können, wie das in einem Geschäft möglich ist (Biswas & Biswas, 2004; Boos, 2015). Zwar können sich Anbieter von Online-Stores im Rahmen der Produktpräsentation bemühen, diese Lücke zu schließen, die Angaben könnten dabei aber auch trotzdem nicht der Wahrheit entsprechen (Boos, 2015), wie das z. B. bei sogenannten Fakeshops der Fall ist. Juristisch führt das zur sogenannten eingeschränkten Entscheidungsfreiheit, die Boos (2015) ausführlich beschreibt. Darüber hinaus kann es dazu führen, dass keine, minderwertige oder gefälschte Ware erhalten wird. Im Weiteren können auch die persönlichen Daten oder das verwendete Geld entwendet werden (Bitkom, 2017a; Polizei Niedersachsen, o.D.). Weiterhin besteht die Gefahr von langwieriger Kommunikation, zusätzlichen Kosten oder nicht getätigten Erstattungen (Boos, 2015). Laut Kim, Xu & Gupta (2012) nimmt der Betrug an Kunden durch Internetverkäufer zu. Ohne direkt mit dem Anbieter interagieren zu können, fällt es Nutzern schwer, dessen Glaubwürdigkeit einzuschätzen (Biswas & Biswas, 2004). Es liegt demnach ein Informationsdefizit und somit Unsicherheit auf Seiten der Nutzer vor (Ahrholdt, 2010). An der Stelle sei erwähnt, dass Unsicherheit aber vermutlich auch bei Zugang zu vollständiger Information vorliegen würde, da der Nutzer laut Acquisti und Grossklags (2005) gar nicht in der Lage wäre, die Menge an Information angemessen zu verarbeiten und optimal zu agieren. Wie bereits in Kapitel 2.1.5 dargestellt führt eine höhere Unsicherheit der Nutzer, in diesem Fall bezüglich Onlineshopping, zu einer Erhöhung des wahrgenommenen Risikos (Biswas & Biswas, 2004). Im Vergleich zu Ladeneinkäufen ist das wahrgenommene Risiko der Nutzer beim Onlineshopping höher (Bhatnagar & Ghose, 2004; Biswas & Biswas, 2004; Jiuan Tan, 1999). Dies und eventuelle Negativerfahrungen können dazu führen, dass die Nutzung verweigert wird (Boos, 2015). Tabelle 1 fasst in der Literatur zu dem Thema gefundene unterschiedliche Arten von Risiko zusammen, die im Folgenden genauer beschrieben werden.

Laut Boos (2015) betreffen die Risiken beim Onlineshopping vor allem das Persönlichkeitsrecht, die Entscheidungsfreiheit, sowie das finanzielle Vermögen der Nutzer. Im Rahmen ihrer Forschung konnten Forsythe und Shi (2003) vier Typen von wahrgenommenen Risiken von Onlinekäufern darstellen. Sie bezeichneten sie als finanzielles, auf die Produktleistung bezogenes, psychologisches und auf den Verlust von Komfort, bzw. Zeit bezogenes Risiko. Forsythe et al. (2006) erarbeiteten einen Fragebogen, um den wahrgenommenen Nutzen und Risiken des Onlineshoppings erfassen zu können. Im Rahmen einer Literaturrecherche und Interviews erarbeiteten sie folgende mögliche Dimensionen von Risiken: Produktqualität; Security; Privacy; Schwierigkeiten im Umgang mit Technologie; Zeitverzögerung; Nicht mit echten Menschen interagieren können; Zusatzkosten; Fehlen von Informationen; Schlechte Erfahrungen und Mangel an Vertrauen in Onlineshopping. Im Rahmen der gründlichen testtheoretischen Untersuchung ihrer Datenbasis erfüllten allerdings nur die drei Dimensionen finanzielles Risiko, Produkt-Risiko und Zeit-Risiko die Kriterien der Fragebogenerstellung.

Tabelle 1. Identifizierte Arten von Risiko im Rahmen von Onlineshopping.

Quelle	**Arten von Risiko im Rahmen von Onlineshopping**
Boos (2015)	Risiko bezüglich Entscheidungsfreiheit Risiko bezüglich Persönlichkeitsrecht Risiko bezüglich Vermögen
Forsythe & Shi (2003)	Finanzielles Risiko *(financial risk)* Auf die Produktleistung bezogenes Risiko *(product performance risk)* Psychologisches Risiko *(psychological risk)* Auf den Verlust von Komfort, bzw. Zeit bezogenes Risiko *(time/convenience loss risk)*
Forsythe et al. (2006)	Finanzielles Risiko *(financial risk)* Produkt-Risiko *(product risk)* Zeit-Risiko *(time/convenience risk)*
Bhatnagar & Ghose (2004)	Produkt-Risiko *(product risk)* Sicherheits-Risiko *(security Risks)*
Biswas & Biswas (2004)	Leistungs-Risiko *(perceived performance risk)* Finanzielles Risiko *(perceived financial risk)* Transaktions-Risiko *(perceived transaction risk)*

Auch Bhatnagar und Ghose (2004) gehen von einem Produkt-Risiko im Rahmen von Onlineshopping aus. Sie begründen das mit der Tatsache, dass Produkte im Vorfeld nicht physisch geprüft werden können. Laut Biswas und Biswas (2004) führt diese Tatsache dagegen zu einem erhöhten Leistungs-Risiko, welches beinhaltet, dass das Produkt nicht funktioniert. Daraus ergibt sich zusätzlich das von ihnen vorgeschlagene finanzielle Risiko. Die dritte Art von Risiko, die sie identifizierten, ist das Transaktions-Risiko, welches sich speziell durch das Internet ergibt und bei traditionellen Ladeneinkäufen nicht vorliegt. Es beinhaltet die Unsicherheit, die sich aus der Preisgabe von Informationen, wie z. B. Kreditkartennummer, Name, Adresse usw. ergibt. Die Informationen werden dabei über ein öffentliches Netzwerk an einen entfernten Empfänger übermittelt, was zu Unsicherheit bezüglich eines potenziellen Missbrauchs der Daten führt (Biswas & Biswas, 2004). Inhaltlich entspricht dieses Risiko dem zweiten von Bhatnagar und Ghose (2004) vorgeschlagenen Risiko, neben dem oben erwähnten Produkt-Risiko. Sie bezeichnen es als Sicherheits-Risiko und verstehen darunter ein Risiko, welches spezifisch für das Internet ist und mit der Angst der Konsumenten zusammenhängt, dass skrupellose Elemente Zugang zu ihrem Account bekommen könnten. Diese spezifische Art von Risiko und weitere Risiken, die sich im Rahmen von Onlineshopping bezüglich der personenbezogenen Daten ergeben, sind in Kapitel 2.2.1 zusammengefasst dargestellt. Entsprechend der Bewertung eines Risikos nach Eintrittswahrscheinlichkeit und potentieller Schadenshöhe (vergleiche Kapitel 2.1.5) werden in den beiden folgenden Kapiteln Daten bezüglich der Wahrscheinlichkeit eines Angriffes auf die personenbezogenen Daten (Kapitel 2.2.2) und sich daraus ergebende potentielle Konsequenzen (Kapitel 2.2.3) dargestellt.

2.2.1 Risiko bezüglich der personenbezogenen Daten im Rahmen von Onlineshopping

Basierend auf Unsicherheiten, die Kaufentscheidungen mit sich bringen, beinhaltet jeder Einkauf ein gewisses Risiko (Biswas & Biswas, 2004). Die zusätzliche Besonderheit in Bezug auf Onlineshopping ist die, dass personenbezogene Daten ausgetauscht werden. Die Preisgabe der personenbezogenen Daten im Internet wird aus mehreren Gründen als riskant angesehen (Youn, 2009). Smith, Milberg und Burke (1996) konnten die Bedenken von Konsumenten bezüglich des Schutzes ihrer persönlichen Daten in vier Gruppen einteilen. Die erste Gruppe stellen die Bedenken bezüglich der Sammlung (*collection*) von personenbezogenen Daten dar. Diese ist eng mit der Gruppe von Bedenken verbunden, bei denen es um die unautorisierte zusätzliche Nutzung (*unauthorized secondary use*) von personenbezogenen Daten geht. Boos (2015) nennt dies das juristische Risiko des unzulässigen Umgangs mit Daten. Denkbar ist hier sowohl eine solche zusätzliche Nutzung durch die Partei, der die Daten auch anvertraut wurden (*unauthorized secondary use* (*internal*)), als auch durch eine dritte Partei (*unauthorized secondary use* (*external*)). So machen es sogenannte Data Mining (*Datengewinnung*) Technologien möglich, dass Anbieter ihre Angebote individuell auf ihre Kunden anpassen (Raman & Pashupati, 2004), um diese damit stärker zu beeinflussen (Wambach, 2017). Spezielle Software, mit der Bewegungen der Nutzer im Internet verfolgt werden kann, ermöglicht es, ohne das Einverständnis oder das Wissen des Nutzers Verhalten und Vorlieben zu überwachen (Olivero & Lunt, 2004). Dabei wird sogar so weit gegangen, dass die so gewonnene Datenbasis mit zusätzlichen Daten, wie z. B. dem entsprechenden Social-Media-Profil in Verbindung gebracht wird, um die Qualität der Daten noch zu steigern (Wambach, 2017). Umgekehrt konnten Olejnik, Castelluccia und Janc (2014) zeigen, dass schon das Wissen um besuchte Webseiten und die IP Adresse ausreichen, um nahezu 70% ihrer Probanden einen einzigartigen „Fingerabdruck“ zuzuordnen, der bei 38% von ihnen sogar über die Zeit stabil blieb. Im Rahmen ihrer Arbeit stellen sie eine Sammlung von Möglichkeiten zum sogenannten *Web fingerprinting* dar, die es möglich machen, einzelne Nutzer z. B. auf Basis ihrer Browserkonfigurationen, verwendeter Schriftarten oder sogar Verhaltensaspekten wie Schreibdynamiken oder Stimmanalysen eindeutig zu identifizieren. Herrmann (Herrmann, 2016) unterscheidet diese Techniken in *Website-* und *Software-Fingerprinting*, wobei bei ersteren das Muster besuchter Webseiten und bei zweiteren Charakteristika der eingesetzten Anwendungen zur Identifikation einzelner Nutzer verwendet werden. Dazu ist es entgegen bisheriger Annahmen sogar möglich Nutzer, trotz wechselnder IP Adressen, über mehrere Tage hinweg zu verfolgen (Herrmann, 2016).

Laut Boos (2015) ergibt sich das Risiko der Verknüpfung und Sammlung umfangreicher Persönlichkeitsprofile aus der heutigen nahezu unbegrenzten Speicherkapazität. Die Nutzerdaten werden dabei entweder durch den Webseitenbetreiber, bzw. den Transaktionspartner selbst weitergegeben oder von einer Drittpartei erlangt (Ahrholdt, 2010; Olivero & Lunt, 2004; Wambach, 2017). Dabei sei erwähnt, dass nicht notwendigerweise ein Vertrag abgeschlossen werden muss, damit personenbezogene Daten beim Anbieter vorliegen (Boos, 2015). Aussagen darüber, inwieweit das systematische „Tracking“ von Nutzerdaten in den letzten Jahren zugenommen hat, können Wambach und Bräunlich (2016) dank ihrer retrospektiven Untersuchung der beliebtesten Webseiten der letzten Jahre machen. Sie konnten nachweisen, dass sich die Zahl der Weitergabe von Nutzerdaten an Drittparteien in den letzten Jahren (2005-2014) verfünffacht hat. Dabei stellen Sie als besonders beunruhigend heraus, dass es sich bei vier von den fünf am häufigsten gefundenen Drittparteien um die gleiche dahinterstehende Firma handelt. Das führt dazu, dass diese in 2015 80% der Internetnutzung überwacht (Wambach & Bräunlich, 2017).

Aber auch ohne eine Weitergabe von Daten besteht die Gefahr, dass bestehende Datenbestände in einem neuen Kontext oder einem neuen Ziel verwendet werden (Wambach, 2017). Wambach (2017, S. 168)

konstatiert dazu: „Wenn bereits heute die Datenbasis für die Algorithmen von morgen gesammelt werden und wir nicht abschätzen können, wie diese Algorithmen aussehen, so muss die Situation bereits heute, zum Zeitpunkt der Datenerhebung, kritisch hinterfragt werden."
Die dritte Gruppe von Bedenken bezüglich des Schutzes der personenbezogenen Daten, die Smith, Milberg und Burke (1996) identifizieren konnten, beschreibt die Befürchtung sich vor vorsätzlichen oder auch versehentlichen Fehlern (*errors*) in den personenbezogenen Daten nicht schützen zu können. Falsch zugeordnete Zahlungsanweisungen oder Willenserklärungen könnten so zu nachteiligen Konsequenzen für eigentlich unbeteiligte Personen führen (Bundesamt für Sicherheit in der Informationstechnik, o.D.a).
Die Befürchtungen, dass die eigenen personenbezogen Daten verfügbar sind für Personen, die nicht dazu autorisiert sind diese zu sehen oder zu bearbeiten, fassen Smith, Milberg und Burke (1996) in der Gruppe des missbräuchlichen Zugriffs (*improper access*) zusammen. Ein Beispiel hierfür stellt das sogenannte Online-Skimming dar. Dabei werden schädliche Programmcodes durch Sicherheitslücken in die Software von Webshopbetreibern implementiert, welche die Zahlungsinformationen der Kunden auslesen und übermitteln (Bundesamt für Sicherheit in der Informationstechnik, 2017b). Dieser Vorgang ist für den jeweiligen Nutzer nicht erkennbar (Bundesamt für Sicherheit in der Informationstechnik, 2017b). Laut des Bundesamtes für Sicherheit in der Informationstechnik (2017b) wird Online-Skimming durch die oftmals nachlässige Absicherung der Dienste durch die jeweiligen Betreiber ermöglicht.

2.2.2 Wahrscheinlichkeit für Angriffe auf personenbezogene Daten im Rahmen von Onlineshopping

Aussagekräftige Quellen dazu zu finden, wie wahrscheinlich Angriffe auf persönlichen Daten im Rahmen von Onlineshopping sind, ist sehr schwierig. Besonders der in Kapitel 2.2.1 dargestellte Fall des Trackings von Nutzerdaten, der sich in den letzten Jahren zu einem ernsthaften Problem entwickelt hat (Wambach & Bräunlich, 2016), ist schwierig zu beziffern. Im Rahmen dieses Kapitels wird sich deshalb auf tatsächliche Zahlen über Delikte gestützt, die vom Bundeskriminalamt veröffentlicht wurden. Diese werden ergänzt durch Ergebnisse zweier repräsentativer Umfragen, die in den Jahren 2014 und 2017 durchgeführt wurden. Das Bundeskriminalamt meldete im Jahr 2018 eine „steigende Kriminalitätsentwicklung" im Bereich Cybercrime (Bundeskriminalamt, 2018). Als Cybercrime werden dabei Straftaten zusammengefasst, „die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden" (Bundeskriminalamt, 2018). Das private und unabhängige Sozial- und Marktforschungsinstitut infas befragte dazu im Jahr 2014 eine, für die deutsche Bevölkerung repräsentative Stichprobe, von 1508 Personen ab 18 Jahren (infas, 2014). Innerhalb der vorangegangenen zwei Jahre sollen demnach 9 Millionen Deutsche Opfer von Internetbetrug geworden sein. Der breite Begriff des Internetbetrugs wird im Rahmen der Studie nur bedingt konkretisiert. Dargestellte Kategorien, die im Zusammenhang mit Datenschutz beim Onlineshopping relevant sind, stellen der Kreditkartenmissbrauch und der Erhalt einer ungerechtfertigten Abmahnung dar. Während bei ersterem die Zahl mit 600 000 Opfern noch vergleichsweise gering ist, stellt der Erhalt einer ungerechtfertigten Abmahnung mit 11 Millionen Opfern ein Massenphänomen dar.
Die ebenfalls repräsentative Umfrage an 1017 Internetnutzern ab 14 Jahren, die Bitkom Research im Jahr 2017 durchführte stützt die Tatsache, dass die Anzahl der Delikte zunimmt. Hier gaben fast die Hälfte der Befragten (49%) an, im letzten Jahr Opfer von Cybercrime geworden zu sein (Bitkom, 2017a). Während bei 19% der befragten die Zugangsdaten für Online-Dienste, wie Soziale Netzwerke oder

Online-Shops entwendet wurden, wurden in 18% der Fälle die persönlichen Daten illegal genutzt. Betrugsopfer beim Onlineshopping oder Online-Banking waren 16% der Befragten schon mindestens einmal geworden. Nur die wenigsten der Opfer erstatten allerdings daraufhin Anzeige (Bitkom, 2017a). Das führt dazu, dass zwar steigende Fallzahlen im Bereich der polizeilichen Kriminalstatistik festgestellt werden, Experten aber von einer sehr großen Dunkelziffer ausgehen (Bundeskriminalamt, 2018). Laut Bitkom (2017a) stellen dabei Angriffe mit Schadprogrammen, Identitätsdiebstahl und Betrug die häufigsten Delikte dar. Unter Identitätsdiebstahl versteht man dabei die unerlaubte Verwendung einer fremden Identität mit Hilfe von Daten, wie z. B. dem Geburtsdatum, der Anschrift oder der Kreditkartennummern, um beispielsweise soziale Medien, Onlineshopping oder Onlinebanking zu nutzen (Bundesamt für Sicherheit in der Informationstechnik, o.D.a).

2.2.3 Potentielle Konsequenzen von Angriffen auf personenbezogene Daten

Um ein Produkt online kaufen zu können, ist es notwendig personenbezogene Daten mittels des Internets zu transferieren. Diese Daten ergeben ein mehr oder weniger komplettes Bild einer bestimmten Person (Herrmann, 2016). Die Konsequenzen, die sich daraus ergeben können sind schwer vorherzusagen (Wambach & Bräunlich, 2016). Obwohl laut Buxmann (2015) ein Großteil der Nutzer nicht mit einer monetären Nutzung ihrer Daten einverstanden ist, wird z. B. die personalisierte Werbung häufig als Service und nicht als Problem angesehen (Wambach, 2017). Wambach (2017, S. 168) begründet das darin, dass der Einzelne „zunächst keine unmittelbaren Nachteile“ erfährt. Die Kosten, die sich aus der Verletzungen der Privatsphäre der Nutzer ergeben sind generell schwer zu quantifizieren, da sie sowohl monetär als auch immateriell sein können und häufig erst nach einiger Zeit (Acquisti & Grossklags, 2005) oder sogar gar nicht vom Nutzer bemerkt werden (Herrmann, 2016). So können sich nutzerseitig unbemerkt getätigte Bonitätseinschätzungen von Online-Versanddiensten auf das jeweilige Angebot auswirken (Boos, 2015). Das Wissen um bestimmte Charakteristika kann darüber hinaus zu unterschiedlichen Arten der Diskriminierung führen (Herrmann, 2016). So können z. B. auch Verträge verweigert oder Prämien, z. B. von Versicherungen erhöht werden (Herrmann, 2016). Aber auch Angriffe mittels, gezielt auf die jeweilige Umgebung zugeschnittener Schadsoftware, sind auf Basis des in Kapitel 2.2.1 dargestellten *Software-Fingerprintings* möglich (Herrmann, 2016). Die Konsequenzen des sogenannten Identitätsdiebstahls stellen sich häufig in Form von Rufschädigung und einem hohen Zeitaufwand dar um den Schaden zu regulieren (Bundesamt für Sicherheit in der Informationstechnik, o.D.a). Eine bereits in Kapitel 2.2.2 dargestellte Studie von Bitkom Research (2017a) zeigte, dass 50% der Fälle von Cybercrime zu finanziellem Schaden führten. Dieser ergibt sich aus notwendigen Reparaturen, der Neuanschaffung von Hard- oder Software oder Waren, die nicht geliefert oder umgekehrt, auch nicht bezahlt wurden. Weitere finanzielle Folgen, die sich auf den Verlust der Privatsphäre beziehen lassen, stellen Kosten für eingeschalteten Rechtsbeistand, bzw. direkten Verlust durch fremde Transaktionen bezüglich Konto und Kreditkarte dar. Weniger greifbar sind dagegen emotionale Konsequenzen, wie eine Angst überwacht zu werden oder der Verlust der Anonymität (Youn, 2009).

Fazit

Das Internet birgt unterschiedliche Arten von Risiken. Im Rahmen dieser Arbeit wird der Fokus dabei auf eine Art von Risiko gelegt, die einer Kombination aus dem Transaktions-Risiko von Biswas und Biswas (2004) und dem Sicherheits-Risiko von Bhatnagar und Ghose (2004) entspricht. Ersteres

beinhaltet die Unsicherheit, die sich aus der Preisgabe von Informationen ergibt und zweiteres die Angst davor, dass Dritte Zugang zum eigenen Account erlangen können. Beides wird in dieser Arbeit unter dem Risiko für personenbezogene Daten zusammengefasst und auf den Kontext des Online-Shoppings eingegrenzt. Die personenbezogenen Daten können dabei gesammelt, unautorisiert genutzt, mit Fehlern versehen oder darauf missbräuchlich zugegriffen werden (Smith et al., 1996). Steigende Fallzahlen, eine vermutete hohe Dunkelziffer (Bundeskriminalamt, 2017) und 49% von Cybercrime betroffene befragte Nutzer lassen zumindest vermuten, dass die Wahrscheinlichkeit ein Opfer im Rahmen dieses Risikos zu werden nicht unwesentlich ist. Die sich in einem solchen Fall ergebenden Kosten können dabei sowohl monetär, als auch immateriell (Acquisti & Grossklags, 2005) und sogar emotional (Youn, 2009) sein.

2.3 Sicherung des Datenschutzes

Die Nutzung des Internets ohne die Preisgabe von Daten, die der jeweiligen Person in irgendeiner Art zugeordnet werden können, ist nicht möglich (Boos, 2015). Zusätzlich ist es kaum möglich einmal im Internet veröffentlichte Daten wieder vollständig zu löschen (Boos, 2015). Nutzern stehen aber unterschiedliche Mittel zu Verfügung das Risiko bezüglich ihrer personenbezogenen Daten wenigstens möglichst gering zu halten. Unterstützung bietet dabei der Staat. So schützt die Bundesrepublik Deutschland ihre Bürger diesbezüglich mit unterschiedlichen Gesetzen und Verordnungen. Ein grober Überblick darüber ist in Kapitel 2.3.1 dargestellt. Ein tieferes Eindringen in die Materie bieten z. B. Boos (2015), Roßnagel, Geminn, Jandt und Richter (2016) und die Deutschen Gesetzbücher (siehe Kapitel 2.3.1).
Neben der rechtlichen Absicherung bieten unterschiedlichste technische Systeme und Anwendungen dem Nutzer die Möglichkeit, Risiken zu minimieren. Diese Art des Schutzes ist in Kapitel 2.3.2 dargestellt. Den möglicherweise effektivsten Schutz stellt allerdings das generelle sichere Verhalten bei der Nutzung des Internets dar, welches in Kapitel 2.3.3 behandelt wird.

2.3.1 Absicherung durch den Staat

Das Kaufen unterschiedlicher Waren und Güter ist in Deutschland gesetzlich geregelt. Grundsätzlich macht es dabei keinen Unterschied, ob diese Waren online oder beim Einkauf in einem Ladengeschäft erworben werden (Boos, 2015). Der private Käufer (juristisch: Verbraucher) wird dabei gegenüber dem Unternehmer als der schwächere Verhandlungspartner gesehen. Seine Rechte werden deshalb im Rahmen des Verbraucherschutzrechts innerhalb des Bürgerlichen Gesetzbuches geschützt. Dieses beinhaltet umfassende Festlegungen bezüglich Themen wie, z. B. der Übergabe der Ware, bzw. Übertragung des Eigentums mit allen zugehörenden Rechten und Pflichten, Widerrufsrechte und Schuldverhältnisse. Zusätzlich schützen Vorschriften im Rahmen der Preisangabenverordnung, der Anbieterkennzeichnung und der kommerziellen Kommunikation den Verbraucher (Boos, 2015).
Die 2011 verabschiedete neue europäische Verbraucherrichtlinie nimmt sich darüber hinaus den Besonderheiten des Onlineeinkaufs an. So findet sich darin z. B. die sogenannte Button-Lösung. Diese hat zum Ziel, unbewusste oder ungewollte Einkäufe oder Abonnements zu verhindern. Dafür wurde festgelegt, dass ein Einkauf ausdrücklich bestätigt werden muss, indem dafür eine Schaltfläche verwendet wird, die eindeutig und erkenntlich gestaltet ist (Boos, 2015; Polizei Niedersachsen, o.D.).
Der hier interessierende Gegenstand des Datenschutzes findet sich in der Charta der Grundrechte der Europäischen Union (GRCh) aus dem Jahr 2000. Der Schutz der persönlichen Daten ist darin im Rahmen

des Grundrechtes auf Achtung des Privatlebens beschrieben. Im Dezember 1995 trat die europäische Datenschutzrichtlinie (DSRL) in Kraft, die in Deutschland allerdings erst seit dem Jahr 2001 umgesetzt wird (Roßnagel et al., 2016). Sie regelt die Verarbeitung personenbezogener Daten und beinhaltet z. B. eine Informationspflicht gegenüber der betroffenen Person, ein Auskunftsrecht bzw. ein Recht auf Berichtigung, Löschung oder Sperrung personenbezogener Daten (Roßnagel et al., 2016).
Das bedeutendste nationale Recht bezüglich des Datenschutzes stellte bislang das Grundrecht auf Informationelle Selbstbestimmung dar. Dieses begründet sich auf dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983, wobei es aus dem Grundgesetz abgeleitet wurde (Boos, 2015). Das Recht auf informationelle Selbstbestimmung soll verhindern, dass digitale Daten automatisiert weiterverarbeitet werden (Roßnagel et al., 2016). Die Feststellung, Verwendung, Speicherung, Weitergabe und Veröffentlichung der Daten darf nur mit dem Willen der entsprechenden Person erfolgen.
Die informationelle Selbstbestimmung ist im Rahmen des Bundesdatenschutzgesetzes geschützt. Zusätzlich dazu gibt es für jedes Bundesland ein spezifisches Landesdatenschutzgesetz sowie spezifische Vorschriften (Roßnagel et al., 2016). Speziell auf den Kontext von Internetanwendungen zugeschnitten ist das sogenannte Telemediengesetz (TMG) (Boos, 2015). Es regelt z. B., welche Maßnahmen Betreiber von Online-Shops ergreifen müssen, um Nutzerdaten zu schützen (Bundesamt für Sicherheit in der Informationstechnik, 2017b).
Seit dem 25. Mai 2018 gelten alle nationalen Datenschutzgesetze der EU als ersetzt durch die EU-Datenschutz-Grundverordnung. Ziele dieser sind, natürliche Personen bei der Verarbeitung personenbezogener Daten, deren Grundrechte und Grundfreiheiten und den freien Verkehr personenbezogener Daten zu schützen (*Datenschutz-Grundverordnung,* 2018). Dazu beinhaltet sie unter Art. 5 *Grundsätze für die Verarbeitung personenbezogener Daten*. Diese sind Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit und Rechenschaftspflicht (*Datenschutz-Grundverordnung,* 2018).
Häufig kommen Gesetze für den Nutzer allerdings erst dann wirklich zum Tragen, wenn bereits eine Rechtsverletzung stattgefunden hat. Notwendig ist es dann, dass eine entsprechende Anzeige erstattet wird. Die Umfrage von Bitkom (2017a) ergab, dass im Kontakt mit Polizei und Staatsanwaltschaft zwar positive Erfahrungen gemacht wurden, die Anzeige aber nur in 7% der Fälle zur Identifizierung eines Täters führte. Häufig mangelt es an Beweisen (37%) oder es kann kein Täter ermittelt werden (24%) (Bitkom, 2017a). Eine präventive und aktive Möglichkeit des Schutzes der persönlichen Daten stellt dagegen die technische Absicherung dar, die im Folgenden näher dargestellt wird.

2.3.2 Technische Möglichkeiten der Absicherung

Es gibt viele unterschiedliche Möglichkeiten, die eigene Soft- und Hardware vor den generellen Risiken des Internets zu schützen. So vermeiden Firewalls, Anonymisierungsdienste, Antiviren Software und in Bezug auf Sicherheitsupdates aktuell gehaltene und restriktiv konfigurierte Browser und Betriebssysteme unerlaubte Zugriffe auf die eigenen Daten (Herrmann, 2016). Das Bundesamt für Sicherheit in der Informationstechnik (BSI) weist in dem Zusammenhang darauf hin, dass dafür moderne Internet-Browser verwendet werden sollen. Diese verfügen über aktuelle Sicherheits- und Filtermechanismen, die vor schädlichen Webseiten, Phishing und Malware warnen (Bundesamt für Sicherheit in der Informationstechnik, o.D.c). Weiter wird empfohlen, nur Plug-Ins und Add-ons zu verwenden, die unbedingt notwendig sind. Dabei handelt es sich um Zusatzprogramme und Funktionen für den jeweiligen Browser, die gesondert installiert werden (Polizei Niedersachsen, o.D.). Im Falle der Nutzung

einer WLAN- Verbindung besagt ein weiterer Hinweis des BSI, diese immer mit Verschlüsselungsstandard WPA2 zu verschlüsseln (Bundesamt für Sicherheit in der Informationstechnik, o.D.c). Das Bundesamt bietet neben Anleitungen, z. B. zum Einrichten eines solch sicheren WLANS, auch Empfehlungen bezüglich der Browserkonfiguration oder Testmöglichkeiten bezüglich des Sicherheitsstatus des eigenen Computers an (Bundesamt für Sicherheit in der Informationstechnik, o.D.c). In jedem Fall verlangt der sogenannte Selbstdatenschutz den Nutzern ein gewisses technisches Verständnis, zeitlichen Aufwand und eventuelle Einschränkungen bezüglich Ladezeiten und/oder Funktionalität ab (Herrmann, 2016). Unabhängig von verwendeter Sicherheitstechnik ist es aber in dem Fall, in dem online Produkte erworben werden sollen, notwendig eigene Daten preiszugeben (Bundesamt für Sicherheit in der Informationstechnik, o.D.b).
In dem Fall bleibt zum Schutz der persönlichen Daten nur die Möglichkeit den jeweiligen Anbieter sorgfältig auszuwählen und die Daten über eine verschlüsselte Verbindung zu transferieren. Hierbei können einige Browsererweiterungen assistieren, indem sie dem Nutzer bestimmte Informationen zu Verfügung stellen. Mit verschiedenen im Hintergrund wirkenden Heuristiken (z. B. *SpoofGuard* (Chou, Ledesma, Teraguchi, Boneh & Mitchell, 2004)), Backlists von betrügerischen Seiten, die abgefragt werden (Downs et al., 2006) oder durch Algorithmen basierend auf diversen Inhalten der entsprechenden Seite (z. B. *Netcraft* (Netcraft LTD., 2018)) machen sich diese Unterstützungen ein Bild von der Seite, welches sie komprimiert an den Nutzer zurückmelden. Andere Programme, wie z. B. Trusted path (Ye, Smith & Anthony, 2005), unterstützen Nutzer dabei unsichere und sichere Verbindungen zu unterscheiden. So werden von vielen Browsern z. B. sowohl ein https (anstatt nur http) in der Adressleiste als auch ein Schlosssymbol gezeigt, wenn die Verbindung verschlüsselt ist. Die beiden Hinweise scheinen für Nutzer redundante Information darzustellen (Whalen & Inkpen, 2005). Dabei bietet das Schlosssymbol zusätzliche Informationen wie Hinweise auf den Verschlüsselungscode, wenn der Cursor sich darüber bewegt, oder Details zum Zertifikat, wenn ein Doppelklick auf das Symbol erfolgt (Whalen & Inkpen, 2005). Für alle diese Programme und Instrumente gilt, dass auch sie nicht immer sicher sind (Norddeutscher Rundfunk, 2016). Es gibt auch Webseiten, auf denen die Nutzer den jeweiligen Shop auf Sicherheitslücken überprüfen können (MageReport, o.D.). Schlussendlich ist es heute schwer, sich technisch vor Beobachtung zu schützen (Herrmann, 2016). Häufig können entsprechende Instrumente und technische Hilfsmittel nur zusätzliche Informationen anbieten. Diese einfordern oder zumindest wahrnehmen muss alleine der Nutzer. Im Rahmen des sogenannten Selbstdatenschutzes unterstützt die Technik den Nutzer nur dabei, seine Daten selbst zu schützen (Boos, 2015). Darüber hinaus bedarf es einer gewissen Sorgfalt von Seiten des Nutzers, die angebotenen Informationen kritisch zu betrachten (Downs et al., 2006). Dessen Verhalten entscheidet am Ende über die Sicherheit der persönlichen Daten. Aus diesem Grund ist das abschließende Kapitel zum Thema Sicherung des Datenschutzes dem Verhalten gewidmet, welches maßgeblich über die Sicherheit der persönlichen Daten entscheidet.

2.3.3 Sicheres Verhalten

Das Bundesamt für Sicherheit in der Informationstechnik betont in seinem Internetauftritt zum IT Grundschutz, den Risikofaktor, den der Mensch als Nutzer im Internet darstellt (Bundesamt für Sicherheit in der Informationstechnik, o.D.a). Dieser sollte Risiken (er)kennen und verantwortungsvoll handeln. Zusätzlich wird betont, dass dazu spezielles Wissen der Nutzer notwendig ist. Wu, Miller und Garfinkel (2006) kamen in ihrer Studie zu der Erkenntnis, dass die Teilnehmer nicht wirklich wussten, wie sie sich online sicher verhalten können. Hargittai (2007) stellt dar, dass es dafür verschiedener

Schritte bedarf. Zunächst muss den Nutzern bewusst sein, dass es Risiken gibt und sie müssen den Inhalten im Internet mit einer gewissen Skepsis begegnen. Dann müssen sie wissen, wie sie Informationen sammeln können, die sie dabei unterstützen, sich ein Bild bezüglich der Rechtmäßigkeit der Quelle des Materials zu machen. Diese nicht trivialen Unterfangen wären nicht nur beim freien Surfen im Netz, sondern auch bei der Durchsicht ihrer Emails wichtig.
Da im Rahmen von Onlineshopping der Internetauftritt die Schnittstelle zwischen dem jeweiligen Anbieter und den Nutzern darstellt, müssen entsprechende Informationen oder Signale diesem entnommen werden (Ahrholdt, 2010). Solche Orientierungshilfen werden Nutzern im Zuge des Selbstdatenschutzes auf unterschiedlichen Informationsseiten im Internet näher gebracht (Wambach, 2017). Stellvertretend seien an der Stelle die Internetpräsenz der Polizei Niedersachsen (Polizei Niedersachsen, o.D.), sowie der Internetauftritt des Bundesamtes für Sicherheit in der Informationstechnik (Bundesamt für Sicherheit in der Informationstechnik, o.D.b) genannt. Auf den Seiten der Polizei Niedersachsen findet sich der „Ratgeber Internetkriminalität“. Unter anderem werden hier Maßnahmen zum Schutz vor Fakeshops, Tipps zur Verwendung entsprechender Add-Ons und zur Begutachtung von Gütesiegeln auf Internetseiten gegeben. Das BSI stellt unter der Überschrift „Worauf beim Online-Einkauf zu achten ist“ eine relativ umfangreiche Liste von Hinweisen vor, anhand derer sich Nutzer ein Bild bezüglich der Vertrauenswürdigkeit eines Anbieters machen können. Dazu gehören Name und Anschrift des Anbieters, die Allgemeinen Geschäftsbedingungen, Hinweise zu Datenschutz bzw. Datensicherheit usw. Auch woran eine verschlüsselte Verbindung zu erkennen ist oder, dass das Löschen von Cookies die Profilbildung zumindest erschwert, ist darin dargestellt. In Bezug auf die Aneignung von Wissen und die Recherche potentieller Hinweise bemerkt Boos (2015), dass Nutzer dies aufgrund der Zeit, die dafür aufgewendet werden muss, häufig weder können noch wollen. Auf einer weiteren Seite des BSI findet sich unter der Überschrift „Zwölf Maßnahmen zur Absicherung gegen Angriffe aus dem Internet“ der Hinweis, dass Nutzer generell zurückhaltend in Bezug auf ihre persönlichen Daten vorgehen und misstrauisch sein sollten (Bundesamt für Sicherheit in der Informationstechnik, o.D.c). Auch Hargittai (2007) stellt dar, dass die Preisgabe möglichst weniger Informationen essenziell ist um den Schutz sensibler Daten zu gewährleisten.

Fazit

Bei der Nutzung der Internets keine Spuren zu hinterlassen, ist nicht möglich (Boos, 2015). Es gibt jedoch unterschiedliche Möglichkeiten, die preisgegebenen Daten abzusichern. Eine in Bezug auf die Nutzer des Internets eher passive Lösung stellt der Schutz der personenbezogenen Daten dar, der in Deutschland gesetzlich geregelt ist. Hier greifen vor allem das Verbraucherschutzrecht, die Datenschutzrichtlinie und das Grundrecht auf informationelle Selbstbestimmung. Über allem steht dazu seit Mai 2018 die umfassende EU-Datenschutz-Grundverordnung. Aktiv können sich Nutzer auch technisch gegen Risiken in Bezug auf personenbezogene Daten absichern. Hierfür stehen eine Reihe Soft- und Hardwarelösungen, sowie unterschiedliche Portale zu Verfügung, die nützliches Wissen vermitteln und einen gewissen Schutz bieten. Jedoch müssen diese gelesen, bzw. verwendet und aktuell gehalten werden. So stellt letztendlich das (sichere) Verhalten der Nutzer den wesentlichsten Schutz der persönlichen Daten dar.

2.4 Menschliches Verhalten im Kontext von Risiko

Nutzer müssen im Rahmen von Onlineshopping Entscheidungen in einer Situation treffen, die einen Anteil an Unsicherheit und Risiko birgt (vergleiche Kapitel 2.2 und 2.2.1). Zu menschlichem Verhalten

in einem solchen Rahmen existieren unterschiedlichste Theorien und Modelle. Nachfolgend (2.4.1) sind hierzu zunächst generelle, dann auf Risikoverhalten bezogene Theorien und Modelle sowie damit zusammenhängende Einflussfaktoren aufgeführt. Dem folgend wird das bereits erwähnte Phänomen des Privacy Paradoxons genauer dargelegt und Erkenntnisse über den Umgang mit Risiken im Kontext des Internets vorgestellt (Kapitel 2.4.2). Im Anschluss daran werden gefundene Möglichkeiten, ein solches Risikoverhalten im Kontext des Internets, bzw. auch des Onlineshoppings zu erfassen, dargestellt (Kapitel 2.4.3) und verwendete Messgrößen analysiert (Kapitel 2.4.3.1).

2.4.1 Einflussfaktoren auf menschliches Verhalten im Kontext von Risiko

Einflussfaktoren auf menschliches Verhalten sind vielfältig. Bevor die Betrachtung der Einflussfaktoren auf Verhalten im Kontext von Risiko eingeschränkt wird, bietet es sich an, zunächst die wesentlichen Erkenntnisse bezüglich des kontextübergreifenden Verhaltens zu betrachten.

2.4.1.1 Theorien zu menschlichem Verhalten

Zu den wohl bekanntesten Theorien menschlichen Verhaltens zählen die Theorie des überlegten Handelns (TRA, Theory of reasonned action, (Fishbein & Ajzen, 1975)) und die Theorie des geplanten Verhaltens (TPB, Theory of planned behavior, (Ajzen, 1985)).
Im Rahmen der Theorie des überlegten Handelns untersuchten Fishbein & Ajzen (1975) die vier Klassen von Variablen *Annahmen* (*Beliefs*), *Einstellungen* (*Attitudes*), *Intentionen* (*Intentions*) und *Verhalten* (*Behavior*). Unter *Annahmen* verstehen die Autoren die wahrgenommene Wahrscheinlichkeit, dass ein Objekt eine bestimmte Eigenschaft hat. Das Ausmaß an Affekt für oder gegen ein Objekt oder eine Person stellt die Variable *Einstellung* dar. Die *Intention* steht für die subjektive Wahrscheinlichkeit, dass das gefragte Verhalten gezeigt wird. Als *Verhalten* wird die beobachtbare Reaktion der jeweiligen Person verstanden. Fishbein und Ajzen (1975) stellen ausführlich die Messbarkeit und Abgrenzung zwischen den Konstrukten sowie Möglichkeiten der Veränderung dieser dar. Darüber hinaus untersuchten sie systematisch deren Verhältnisse untereinander. Es zeigt sich, dass Annahmen die Basis für die Einstellung gegenüber einem Objekt, anderen Menschen oder einem Verhalten bilden. An der Stelle wird die Variable *subjektive Norm* eingeführt. Darunter wird die Wahrnehmung einer Person darüber verstanden, ob die meisten Menschen, die ihm oder ihr wichtig sind denken, dass er oder sie das gefragte Verhalten zeigen soll oder nicht. Die Einstellung gegenüber einem Verhalten und die subjektive Norm nehmen Einfluss auf die Intention das Verhalten in Zukunft zu zeigen und diese Intention wiederum führt dazu, dass das entsprechende Verhalten gezeigt wird oder nicht. Das sich ergebende Modell ist unter Abbildung 1 dargestellt.

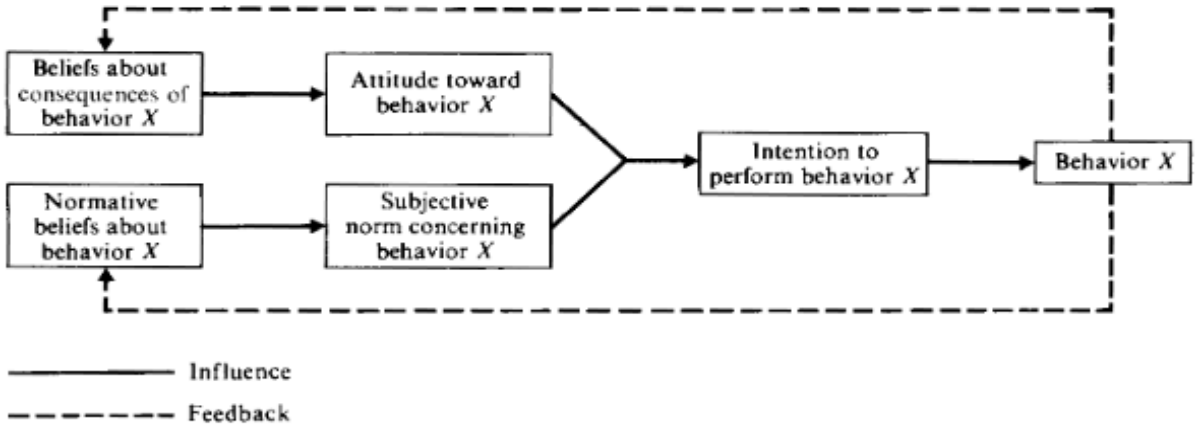


Abbildung 1. Modell der Theorie des überlegten Handelns (Fishbein & Ajzen, 1975).

Die Theorie des überlegten Handelns wurde von Izek Ajzen (1985) zur sogenannten Theorie des geplanten Verhaltens weiterentwickelt. Der wesentliche Unterschied ist die Kontrolle, die eine Person über ihr Handeln hat. Er schreibt, dass das im Rahmen der Theorie des überlegten Handelns verwendete Konstrukt der Intention nur unter zwei Bedingungen direkter Antezedent des jeweiligen Verhaltens ist. Es sind dies die Bedingungen, dass die Messung der Intention dem Verhalten ganz direkt vorangeht und das Verhalten unter volitionaler Kontrolle der Person steht. Das liegt daran, dass sich Intentionen aus unterschiedlichen Gründen ändern können. Ajzen (1985) nennt hier die Zeit, neue Informationen oder dahinter stehende Überzeugungen und Verpflichtungen, die sich ändern können. Darüber hinaus existieren individuelle Unterschiede darin, wie oft man seine Intentionen ändert. Er postuliert, dass jedes beabsichtigte Verhalten ein Ziel darstellt, dessen Erreichung einer gewissen Unsicherheit unterliegt. Er führt im Weiteren Charakteristika, bzw. internale Faktoren aus, die einen Einfluss auf die Zielerreichung haben. Diese sind individuelle Unterschiede bezüglich der Fähigkeit zur *Kontrolle über die eigenen Handlungen* (*behavioral control*), unterschiedliche Informationen, Fähigkeiten und Fertigkeiten, Willensstärke, Emotionen und Zwänge. Als externale Faktoren nennt er Zeit und Möglichkeiten und die Abhängigkeit von anderen. Zusammenfassend gibt er den Hinweis, dass Verhaltensintentionen am besten als *Intention zu versuchen das jeweilige Verhalten zu zeigen* angesehen werden sollen und nicht als tatsächliche Durchführung. Die Frage der Kontrolle ist dabei häufig mit der Entwicklung eines angemessenen Plans verbunden. Dieser Plan beinhaltet ein Set an Intentionen, die, wenn sie durchgeführt werden, in dem gewünschten Verhaltens-Ziel resultieren. Darüber hinaus kann der Plan auch Alternativen enthalten, falls die geplante Sequenz von Verhalten blockiert wird. Die frühere Theorie des überlegten Handelns findet sich in seiner Theorie des geplanten Verhaltens als Spezialfall wieder. Sie gilt nur dann, wenn sowohl die subjektive Wahrscheinlichkeit für Erfolg, die wahrgenommene Kontrolle und der Grad an tatsächlicher Kontrolle über das Erreichen des Ziels ihre Maxima erreichen. Abbildung 2 zeigt das sich ergebende Modell.

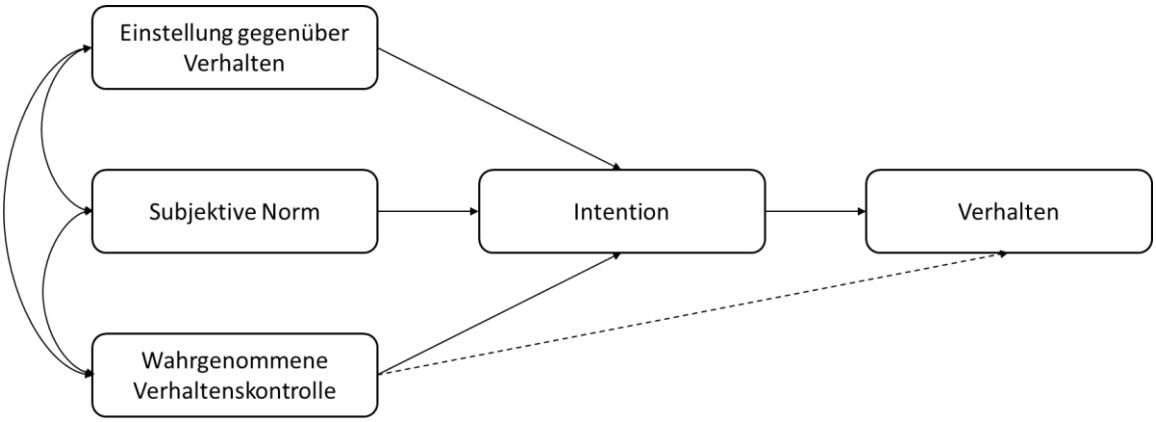


Abbildung 2. Darstellung der Theorie des geplanten Verhaltens (Ajzen, 1985, nach eigener Darstellung).

Tatsächliche Kontrolle ist das, was Risikosituation gerade nicht beschreibt. Wie bereits in Kapitel 2.1.5 beschrieben, beinhalten Risikosituationen Unsicherheiten bezüglich des möglichen Ausgangs. Wie sich Menschen in genau solchen Situationen verhalten, darüber gibt es zusätzliche unterschiedliche Theorien.

2.4.1.2 Theorien zu menschlichem Risikoverhalten

Die Expected Utility Theory von Bernoulli (1954), die ursprünglich aus dem Jahre 1738 stammt, ist dabei eine der ältesten und bekanntesten. Hierin erklärt er, dass Entscheidungen in Situationen in Unsicherheit mathematisch berechnet werden, indem mögliche Gewinne mit ihrer jeweiligen Auftretenswahrscheinlichkeit multipliziert werden und die Summe der Produkte dann durch die Gesamtzahl möglicher Fälle geteilt wird, wenn alle Fälle gleich wahrscheinlich sind. Er kritisiert, dass dabei die Unterschiedlichkeit der Menschen nicht berücksichtigt wird. Diese beurteilen Risiken anders und haben andere Bedürfnisse und Wünsche. Sein Beispiel von einem Lotterielos, mit dem entweder nichts oder 20.000 Dukaten gewonnen werden können, verdeutlicht dies. So werden die Wahrscheinlichkeiten von einem armen Mann ganz anders bewertet werden als von einem reichen Mann. Ein weiteres gutes Beispiel stammt von Byrnes et al. (1999), die darstellen, dass die Möglichkeit Süßigkeiten zu verlieren einem Erwachsenen trivial erscheint, für ein Kind aber höchst unerwünscht wäre. Bernoulli (1954) postuliert deshalb, dass der Wert einer Option weniger nach dem Preis, als vielmehr nach dem Nutzen für die jeweilige Person determiniert werden soll, um solche Unterschiede mit einzubeziehen.
Die Psychologen Daniel Kahneman und Amos Tversky kritisierten diese Theorie 1979 (Kahneman & Tversky, 1979). Sie hatten einige Auffälligkeiten im Verhalten von Menschen im Zusammenhang mit Entscheidungen unter Risiko feststellen können, die sich nicht damit vereinen ließen. Zum einen ordnen Menschen Ausgängen, die als sicher gelten, höhere Gewichte zu im Vergleich zu Ausgängen, die nur wahrscheinlich sind. Dieses Phänomen nennen sie *certainty effect*. Es hängt mit dem von ihnen beobachteten Phänomen zusammen, dass Menschen bei Entscheidungen, bei denen sichere Gewinne möglich sind, sich risikoavers verhalten. Bei Entscheidungen, bei denen sichere Verluste möglich sind, verhalten sie sich dagegen risikofreudig. Darüber hinaus konnten Kahneman und Tversky beobachten, dass Menschen Komponenten, die in allen Optionen enthalten sind verwerfen, was dazu führt, dass sie sich inkonsistent entscheiden, wenn ihnen ein und dieselbe Auswahl auf unterschiedliche Art dargestellt wird. Sie nennen das den *isolation effect*. Im Anschluss an ihre begründete Kritik stellen die beiden Forscher eine alternative Theorie, nämlich die sogenannte Prospect Theory dar. Eine wesentliche Änderung ist dabei die Annahme eines Referenzpunktes von welchem aus Optionen als Gewinne oder

Verluste bewertet werden. Darüber hinaus werden die jeweiligen Wahrscheinlichkeiten durch Entscheidungsgewichte (*decision weights*) ersetzt. Es ergibt sich eine Wertefunktion, die konkav im Bereich der Gewinne und konvex im Bereich der Verluste verläuft. Im Bereich der Verluste verläuft sie zusätzlich steiler als im Bereich der Gewinne.

Motivationale Theorien zu Risikoverhalten

Inhalt der beiden vorangegangenen Theorien sind Entscheidungssituationen, die überwiegend im monetären Kontext verwendet werden. Die sogenannte Protection Motivation Theory von Rogers (1975) beschäftigt sich dagegen mit einer körperlichen Komponente, nämlich der Angst. Laut dieser Theorie gibt es drei wesentliche Komponenten der Angst: das Ausmaß an Schaden, den ein Ereignis hervorrufen würde, dessen Auftretenswahrscheinlichkeit und die Effizienz einer schützenden Reaktion. Die drei Komponenten initiieren einen kognitiven Prozess, der eine Motivation sich zu schützen hervorrufen kann. Ist diese Motivation ausreichend groß, führt sie zu einer Änderung des Verhaltens. Dabei sind die auslösenden Komponenten multiplikativ. Wird ein Event nicht als schädlich oder als unwahrscheinlich eingeschätzt, oder, wenn es nichts gibt, was dagegen getan werden kann, dann entwickelt sich auch keine Schutz-Motivation und das Verhalten ändert sich nicht. Die Protection Motivation Theory ist auf Abbildung 3 dargestellt.

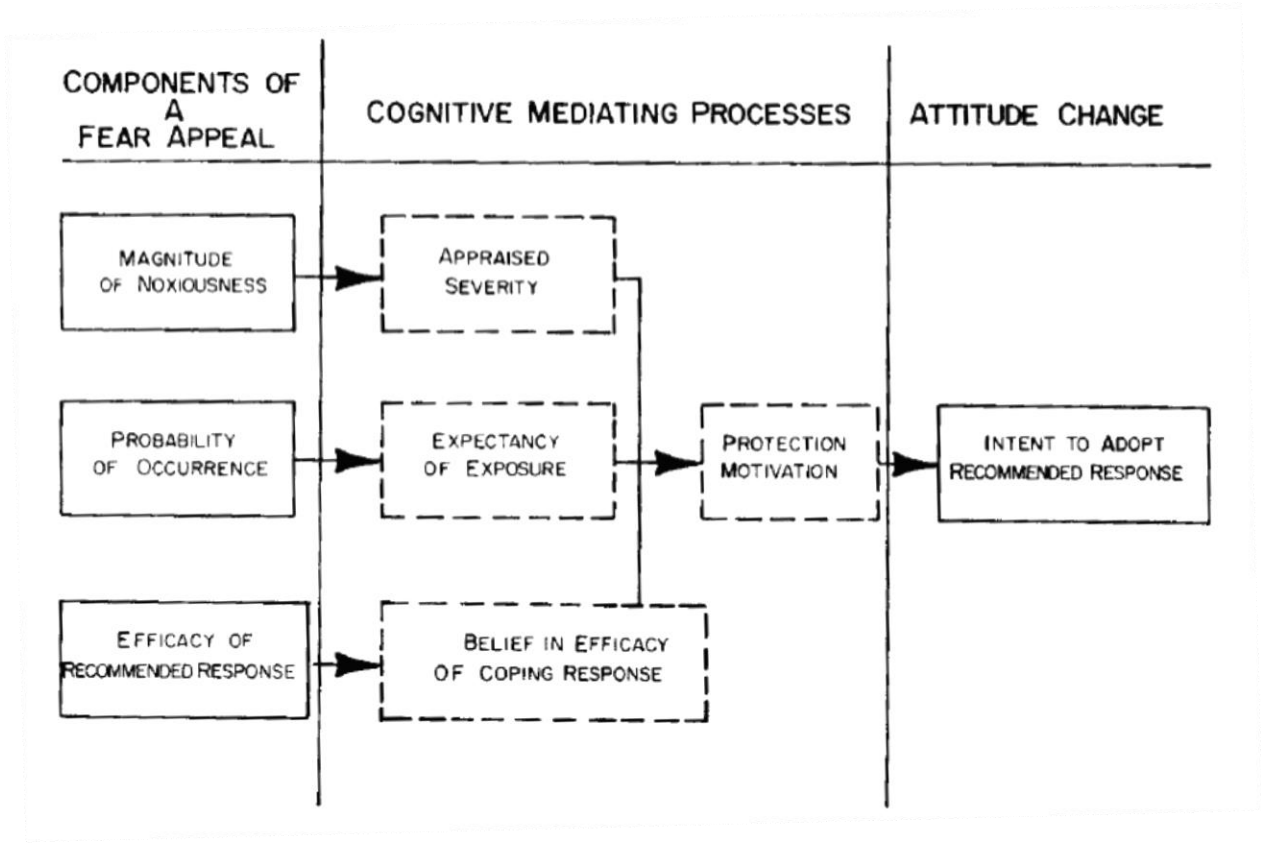


Abbildung 3. Modell der Protection Motivation Theory von Rogers (1975).

Rogers (1975) schränkt seine Darstellung dahingehend ein, dass sie nur die zentralen Prozesse darstellt, da Individuen bedrohliche Ereignisse individuell beurteilen. Darüber hinaus erwähnt er, dass die kognitive Bewertung einer Bedrohung oder Angst voraussetzt, dass die Bedrohung überhaupt wahrgenommen und verstanden wurde.

Ganz ähnlich lautete auch schon der Ansatz von Atkinson (1957) bezüglich motivationaler Einflussfaktoren auf Risikoverhalten. Er stellt dar, dass die Stärke der Motivation eine multiplikative Funktion der Stärke des Motivs, der Erwartung, bzw. der subjektiven Wahrscheinlichkeit davon ist, dass als Konsequenz ein gewisser Anreiz erreicht wird und des Wertes, den dieser Anreiz darstellt (Motivation $= f$ (Motiv x Erwartung x Anreiz)). Das Motiv ist in dem Fall als eine dispositionale Fähigkeit zur Zufriedenheit bei der Erreichung einer bestimmten Art von Anreizen definiert. Werden sowohl eine Motivation sich dem Risiko zu nähern, als auch die das Risiko zu vermeiden angesprochen, so ist die resultierende Motivation die Summe beider Motivationen. Aus einem Set von Alternativen wird die Handlung gezeigt, deren resultierende Motivation am positivsten ist. Die Risikosituationen beschränken sich im Rahmen des Risikowahl-Modells (Wirtz, 2014) von Atkinson allerdings auf Erfolg vs. Misserfolg bei der Bearbeitung einer Aufgabe.

2.4.1.3 Die Verrechnung von wahrgenommenem Risiko mit dem erwarteten Nutzen

Auf eine breitere Auswahl von Risikosituationen wurde bereits das sogenannte Risk-Return Framework von Weber et al. (2002) angewendet. Hier wird die Präferenz einer Person in Bezug auf eine Entscheidung unter Risiko durch eine Funktion des erwarteten Nutzens und dem wahrgenommenen Risiko beschrieben. Während ein steigender erwarteter Nutzen die Bereitschaft für ein risikoreiches Verhalten erhöht, sollte diese bei steigendem wahrgenommenen Risiko sinken (Figner & Weber, 2011). Es ergibt sich folgende Funktion:

$$(1)\ \text{Präferenz (X)} = \alpha\ (\text{Erwarteter Nutzen (X)}) + b\ (\text{Wahrgenommenes Risiko (X)}) + c$$

Die jeweilige Beurteilung der beiden Prädiktoren ist dabei abhängig sowohl von der jeweiligen Situation, als auch des Individuums (Sitkin & Pablo, 1992; Sitkin & Weingart, 1995). Der Zusammenhang der beiden Variablen wurde mit Hilfe der von Weber et al. (2002) entwickelten und von Blais & Weber (2006) überarbeiteten Domain-Specific Risk-Taking (DOSPERT) Scale mehrfach in unterschiedlichen Kontexten nachgewiesen. Im Original unterscheidet der Fragebogen zwischen fünf, bzw. sechs unterschiedlichen Arten von Risiko, den sogenannten Risikodomains *Sozial (Social)*, *Ethik (Ethical)*, *Freizeit (Recreational)*, *Gesundheit & Sicherheit (Health/Safety)* und *Finanzen (Financial)*. Es zeigte sich allerdings im Rahmen erster Studien, dass sich die Risikodomain *Finanzen* in zwei Subdomains aufspaltet. Das Kriterium hierfür ist, ob es sich um eine Situation handelt, deren Ausgang durch Faktoren bestimmt wird, die außerhalb der Person liegen, also z. B. durch Zufall oder ob zusätzliche Informationen oder ein mehr an Fähigkeiten/Fertigkeiten das Risiko verringern können. Ein Beispiel für den ersten Fall stellt klassisch das Glückspiel (*Gambling*) dar, wonach diese Domain deshalb benannt wurde. Den Namen für den zweiten Fall gab das Beispiel einer Investition in eine bestimmte Aktie (*Investing*). Selbst wenn die empfundene Kontrolle und Handhabbarkeit der Situation nur eine illusorische sein sollte, ergeben sich daraus Unterschiede in Bezug auf die Wahrnehmung des Risikos (Weber et al., 2002).
Im Rahmen vieler Studien konnten so Unterschiede im Eingehen von Risiken abhängig vom jeweiligen Risiko (Hanoch, Johnson & Wilke, 2006; Harris, Jenkins & Glaser, 2006; Johnson, Wilke & Weber, 2004; Weber et al., 2002), vom erwarteten Nutzen (Harris et al., 2006; Weber et al., 2002), den Risikodomains (Blais & Weber, 2006; Hanoch et al., 2006; Weber et al., 2002) oder zwischen spezifischen Gruppen (Harris et al., 2006; Weber & Hsee, 1998; Wilke, Hutchinson, Todd & Kruger, 2006) nachgewiesen werden. Darüber hinaus wird das Instrument in anderen Kontexten, wie z. B. bei neurowissenschaftlicher Forschung (Brown & Braver, 2007) verwendet.

Risiko vs. Nutzen im Kontext des Internets

Wenn auch mit anderen Instrumenten als der DOSPERT Scale erhoben, konnten besonders das wahrgenommene Risiko und der erwartete Nutzen auch im hier interessierenden Kontext des Internets als Einflussfaktoren auf Risikoverhalten nachgewiesen werden. So konnten Sunshine et al. (2009) zeigen, dass die Risikowahrnehmung der ausschlaggebende Faktor in Bezug auf die Entscheidung der Probanden war, ob sie eine Webseite besuchen, die potentiell nicht verschlüsselte Daten überträgt. Als gute Prädiktoren erwiesen sich das wahrgenommene Risiko und der erwartete Nutzen in Bezug auf die Intention online einzukaufen (Forsythe et al., 2006) und die Intention sich sicher zu verhalten (Hardee et al., 2016). Für einen erwarteten Nutzen sind Menschen auch bereit, ihre personenbezogenen Daten anzugeben (Norberg et al., 2007). Wichtig ist dabei allerdings auch der Kontext, auf den sich das jeweilige Risiko bezieht. So wird z. B. in Bezug auf Finanzen generell eher eine Risikominderung angestrebt, während in anderen Bereichen ein gewisses Risiko von manchen Menschen als positiv empfunden wird (Weber, 1997). Dagegen scheint das wahrgenommene Risiko eine größere Rolle zu spielen, wenn es um Leib und Leben geht, als um Geld (Hanoch et al., 2006).
Miyazaki & Fernandez (2001) stellen begründet dar, dass der Einfluss des wahrgenommenen Risikos als Prädiktor für Onlineshopping strittig ist. Laut Hardee et al. (2016) hat die Wahrnehmung des Risikos einen großen Einfluss bei Entscheidungen, die Computer betreffen, während die Gewinn-Verlust-Ratio einen größeren Einfluss auf Entscheidungen hat, die nichts mit dem Computer zu tun haben. Da Menschen unterschiedliche Motivationen haben ist es zudem sowieso nicht möglich, Risikoverhalten gänzlich durch den erwarteten Nutzen und das wahrgenommene Risiko zu erklären (Hanoch et al., 2006).

2.4.1.4 Gruppenunterschiede bezüglich des Risikoverhaltens

Unterschiedliche Studien konnten Unterschiede zwischen Gruppen in Bezug auf der Risikobewertung nachweisen. So führten Fogg et al. (2001) eine Studie mit über 1400 Versuchspersonen durch, welche die Vertrauenswürdigkeit von Webseiten einschätzen sollten. Es ergab sich, dass die Personen, abhängig von ihrem Alter, ihrem Geschlecht, Kultur, Bildung und Einkommen sich dabei an unterschiedlichen Merkmalen der Seite orientierten.

Unterschiede in Abhängigkeit des Alters

Die Gruppe der jüngeren Probanden achtete in der Studie von Fogg et al. (2001) eher darauf, ob die entsprechende Seite regelmäßig auf den neuesten Stand gebracht wird, sowie dass keine Schreibfehler und nicht funktionierende Links vorhanden sind. Die älteren Probanden schätzten dagegen eher die Seiten als vertrauenswürdig ein, die von Organisationen stammen, die auch außerhalb des Internets respektiert werden, die wenige Stories aber detailliertere Informationen bieten oder zu anderen Seiten verlinkt sind, denen man vertraut, bzw. die von einer vertrauenswürdigen Person empfohlen wurden. Darüber hinaus wurde die Möglichkeit der Anpassung der Seite an den Nutzer, z. B. in Gestalt von an Präferenzen angepassten Inhalten, von dieser Gruppe als positiv empfunden. Auch eine repräsentative Befragung des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die 2017 durchgeführt wurde konnte aufzeigen, dass die Generationen bezüglich Sicherheit und Seriosität von Online-Shops auf unterschiedliche Merkmale achten (Bundesamt für Sicherheit in der Informationstechnik, 2017a).

Unterschiede in Abhängigkeit des Geschlechts

Nach Teilung der Stichprobe bezüglich der Geschlechter, zeigte sich in der Studie von Fogg et al. (2001), dass die Vertrauenswürdigkeit generell von männlichen Teilnehmern niedriger eingeschätzt wurde als von den weiblichen. Die Autoren begründen dies damit, dass Männer in Fragebögen generell kritischer antworten würden als Frauen.
Johnson et al. (2004) konnten, wie auch schon Weber et al. (2002) zeigen, dass eine unterschiedliche Wahrnehmung des Risikos abhängig vom Geschlecht der Probanden zu Unterschieden im Risikoverhalten führte. In der Studie von Hanoch et al. (2006) zeigte sich dagegen der erwartete Nutzen als auschlaggebenderer Faktor. Auch diesbezüglich fanden Weber et al. (2002) Unterschiede zwischen den Geschlechtern. So erwarteten sich die Männer einen größeren Nutzen als die Frauen bezüglich risikoreicher Aktivitäten in den Domains Finanziell, Gesundheit & Sicherheit, Freizeit und Ethik. In Bezug auf Risikoverhalten in der Domain Sozial war dies umgekehrt der Fall.
Auf Basis ihrer Meta-Analyse von 150 Studien zum Risikoverhalten unterstellten Byrnes et al. (1999) Männern und Jungs einen offensichtlichen Mangel an Einsicht. So gingen sie größere Risiken ein, auch wenn klar ersichtlich war, dass das „keine gute Idee war“ (S.378). Das Gegenteil war bei den weiblichen Teilnehmerinnen der Fall. Diese schienen auch in harmlosen Situationen abgeneigt, Risiken einzugehen. Die Unterschiede zwischen den Geschlechtern variierten zusätzlich mit dem Alter der Probanden. Einige Unterschiede (z. B. in Bezug auf Autofahren) nahmen mit dem Alter zu, während in Bezug auf andere Situationen, wie z. B. beim Rauchen, in allen Altersstufen nur geringe Unterschiede vorherrschten. Unterschiede in Bezug auf Risikoverhalten, die mit dem Alter zusammenhängen, werden oft mit steigenden Erfahrungen und Wissen in Verbindung gebracht.

Unterschiede in Abhängigkeit der Qualifikation, bzw. Erfahrung

Hochqualifizierte Menschen scheitern seltener als Ungelernte an Aufgaben, für welche die entsprechenden Fähigkeiten relevant sind, was bedeutet, dass auf Fähigkeiten bezogene Risikosituationen nur für Zweitere riskant sind (Byrnes et al., 1999). Die damit zusammenhängende Unterscheidung von Experten und Novizen ist eine, die besonders im hier interessierenden Kontext von Computer und Internet häufig untersucht wird. So konnten Miyazaki & Fernandez (2001) Zusammenhänge zwischen dem Level an Erfahrung von Online-Konsumenten, der Nutzung alternativer Shopping-Methoden, wie z. B. per Telefon oder Mailorder, den wahrgenommenen Risiken von Onlineshopping und den online Einkaufsaktivitäten nachweisen. Forsythe et al. (2006) kamen auf Basis ihrer Untersuchung zu dem Schluss, dass Risikobedenken mit steigender Onlineshoppingerfahrung abnehmen, während der erwartete Nutzen zunehmend relevant wird. Bhatnagar & Ghose (2004) konnten nachweisen, dass sich mit zunehmendem Alter und Erfahrung der Nutzer das Risiko, welches in Bezug auf die Attribute des Produktes wahrgenommen wird, verringert. Bravo-Lillo et al. (2011) postulieren, dass weniger erfahrene Nutzer die Sensitivität der Informationen, die sie im Internet angeben, nicht berücksichtigen und deshalb leichter Opfer von Internetkriminalität werden. Darüber hinaus würden sie die Sicherheit einer Handlung erst im Nachhinein bewerten, während fortgeschrittene Nutzer dies im Vorfeld tun. Als weiteren Unterschied geben sie an, dass weniger erfahrene Nutzer weniger Faktoren in ihre Entscheidungen einbeziehen und weniger tun, um ihre Sicherheit zu gewährleisten. In der Studie von Sunshine et al. (2009) konnten sie dagegen nur geringe Unterschiede zwischen Experten und Novizen feststellen. Als möglichen Grund dafür gaben sie an, dass ihr Messverfahren zur Abgrenzung zwischen Experten und Novizen eventuell verbessert werden muss. Sie benutzten dafür fünf Fragen, nämlich, nach einem Abschluss in einem IT-nahen Feld, einem Beruf, der mit Computersicherheit zu tun hat, Erfahrungen oder Lehrveranstaltungen, dem Beherrschen einer

Programmiersprache und der Teilnahme an einer Computersicherheits-Konferenz innerhalb der letzten zwei Jahre. Bei Bravo-Lillo et al. (2011) waren die Kriterien, die Teilnahme an wenigstens einer Hochschulveranstaltung zu Computer oder Datensicherheit oder die Arbeit in einem entsprechenden Projekt im letzten Jahr. Egelman et al. (2008) fragten die Teilnehmer ihrer Studie, ob diese jemals eine Webseite gestaltet, einen Domainnamen registriert, jemals SSH benutzt oder eine Firewall konfiguriert haben. Miyazaki und Fernandez (2001) nutzten Fragen nach der Dauer der Internetnutzung in Jahren und Monaten, die Anzahl der Tage pro Monat, in der ein Browser verwendet wurde, um Zugang zum Internet zu erlangen, und an denen Emails empfangen oder gesendet wurden zur Einordnung ihrer Probanden. Damit konnten sie nachweisen, dass je höher die Interneterfahrung war, desto niedriger war das wahrgenommene Risiko bezüglich Onlineshopping, was sich wiederum in mehr online Käufen niederschlug. Downs et al. (2006) schätzten die Erfahrung der Teilnehmer daran ein, ob sie jemals Einstellungen ihres Browser vorgenommen haben, jemals eine Webseite erstellt oder jemandem dabei geholfen haben ein Computerproblem zu lösen. Sie waren allerdings explizit auf der Suche nach Probanden mit möglichst wenig Kenntnissen. Sollte jemand eine der Fragen bejaht haben, wurde entsprechend nachgefragt und sollte die Antwort mit Datensicherheit zu tun haben, wurde diese Person von der Teilnahme ausgeschlossen. Sie konnten mit ihrer Studie, die in Kapitel 2.4.3 näher beschrieben ist, nachweisen, dass auch naive Nutzer sich in Bezug auf ihre Entscheidungsstrategien unterscheiden.

Unterschiede in Abhängigkeit des Bewusstseins und der Kenntnisse

Die kontinuierliche Entwicklung des Internets führt dazu, dass immer mehr Informationen den Nutzern zur Verfügung stehen (Hargittai, 2005). Diese finden sich deshalb immer häufiger in Situationen wieder, in denen sie Entscheidungen ohne vorheriges Wissen treffen müssen (Wang et al., 2004). Um seine persönlichen Daten in dem Kontext zu schützen, muss zunächst erkannt werden, dass überhaupt eine Gefahr besteht und dann muss das Know-How vorhanden sein, wie dies bewerkstelligt werden kann (Hargittai, 2007). Sind sich die Nutzer nicht bewusst, was passieren kann, so verhalten sie sich weiterhin unsicher (Hargittai, 2007). Allein, dass sie sich dessen bewusst sind, bedeutet allerdings nicht, dass sie sich auch verwundbar fühlen (Downs et al., 2006). Dieser Unterschied zwischen dem Wissen um eine Gefahr und dem entsprechenden Verhalten zeigt sich, laut Rhee, Ryu und Kim (2005), in „einer der wichtigsten Untersuchungen zu Informationssicherheit“ (S.382). So stellte sich in der Studie von Ernst & Young (2004; nach Rhee et al., 2005) dar, dass Manager zwar das fehlende Bewusstsein der Nutzer als das größte Hindernis für Informationssicherheit nennen, aber nur die wenigsten bereit sind, dieses zu verbessern bzw. Trainings anzubieten. Die Nutzer, die sich der Gefahren nicht bewusst sind, werden sich auch nicht mit entsprechenden Mitteln schützen (Downs et al., 2006). Darüber hinaus scheint es auch an nützlichen Strategien zu mangeln. So kamen Acquisti & Grossklags (2005) zu dem Ergebnis, dass sich sogar ihre technologisch versierte und gebildete Stichprobe wenig in Bezug auf technische und juristische Möglichkeiten, die persönlichen Daten im Internet zu schützen, auskannten. Downs et al. (2006) konnten zeigen, dass die Strategien ihrer weniger erfahrenen Nutzer zum Teil auf gemachten Erfahrungen basierten. Die Tatsache, dass diese Strategien nicht wirklich effektiv sind, begründen sie mit einem fehlenden grundlegenden Verständnis des Internets. Auch Buxmann (2015) begründet das bereits beschriebene Privacy Paradoxon (vergleiche Kapitel 1.1) neben fehlender Motivation mit mangelnder Kompetenz. Laut Weber et al. (2002) verändert allerdings auch schon die nur wahrgenommene Fähigkeit mit dem Risiko umgehen zu können das wahrgenommene Risiko in der Situation.

Der Einfluss weiterer personenbezogener Einflussfaktoren auf Risikoverhalten

Weitere personenbezogene Einflussfaktoren auf das Risikoverhalten stellen die gemachten Erfahrungen, die Bildung, das Einkommen und die Nutzungsgewohnheiten dar. So postulieren Miyazaki & Fernandez (2001), dass negative Erfahrungen zu einer verminderten Nutzung von Onlineshopping führen. Die Einstellung der Probanden bezüglich Datenschutz unterschied sich zwischen den Gruppen mit hohem und niedrigem Einkommen bei Acquisti & Grossklags (2005). Dass sich das wahrgenommene Sicherheitsrisiko mit höherer Bildung verringert, konnte von Bhatnagar & Ghose (2004) nur teilweise betätigt werden. Dagegen brachte die bereits in Kapitel 2.2.2 dargestellte Studie des Sozial- und Marktforschungsinstitutes infas die Erkenntnis, dass weniger gebildete Internetnutzer häufiger Opfer von Internetkriminalität wurden als hochgebildete (infas, 2014). Eine Steigerung der Wahrscheinlichkeit dessen ergab sich auch bei steigender Nutzung (infas, 2014).

2.4.1.5 Modell zur Vorhersage des Öffnens eines Emailanhanges

Nahezu alle der im Rahmen dieses Kapitels dargestellten Erkenntnisse sind im Modell von Pfeiffer, Theuerling und Kauer (2013) zusammengefasst (siehe Abbildung 4). Ziel dieses Modells ist die Erklärung, bzw. Vorhersage der Handlung „Öffnen eines Email-Anhanges“. Es umfasst eine umfangreiche Zusammenstellung möglicher Einflussfaktoren, die im Zuge der besseren Darstellung zu Variablengruppen zusammengefasst wurden.

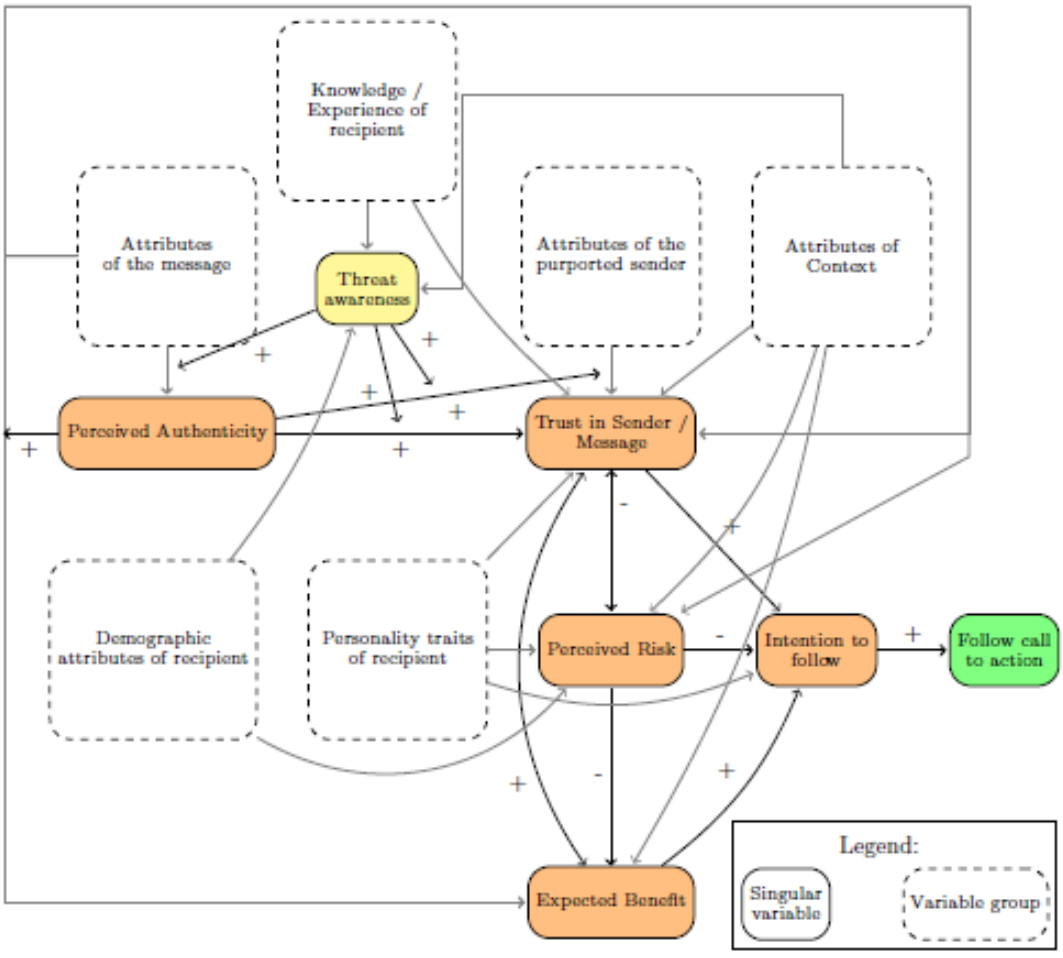


Abbildung 4. Modell zur Vorhersage des Öffnens eines Emailanhanges von Pfeiffer et al. (2013).

Das vorherzusagende Verhalten ist generell mit dem *Folgen einer Handlungsaufforderung*, wie eben dem Öffnen eines Emailanhanges, benannt. Entsprechend den oben beschriebenen Theorien zu menschlichem Verhalten (TRA (Fishbein & Ajzen, 1975) und TPB (Ajzen, 1985)) geht diesem die entsprechende *Intention* voraus. Zur Bildung der *Intention* tragen drei wesentliche Faktoren bei. So wird sie zum einen positiv durch das *Vertrauen* der potentiell handelnden Person in den Sender der Email und die Email selbst beeinflusst. Zum anderen wirkt, wie oben beschrieben, der *erwartete Nutzen* positiv und das *wahrgenommene Risiko* negativ auf die Intention (Forsythe et al., 2006; Hardee et al., 2016). Das *Vertrauen* und das *wahrgenommene Risiko* beeinflussen sich gegenseitig negativ. *Vertrauen* wirkt positiv auf den *erwarteten Nutzen*, der durch das *wahrgenommene Risiko* wiederum negativ beeinflusst wird. Als wichtigste Variablen-Gruppe, die auf die bislang genannten Variablen, Einfluss nimmt, nennen die Autoren die *Eigenschaften der Email* selbst. Darin sind Faktoren, wie die eigentliche Handlungsaufforderung, der Kontext, in den sie eingebettet ist, die Art der Ansprache, sowie die „erzählerische Kraft“, aber auch formale Aspekte wie Design oder Rechtschreibung und das Vorhandensein von Gütesiegeln zusammengefasst. Eine weitere wichtige Gruppe stellen die *Eigenschaften des Senders* der Email dar, die sich an der Reputation, einer Marke oder des Grads an Vertrautheit, Gleichheit oder dem Geschlecht festmachen lassen. Um individuelle Unterschiede bezüglich Vertrauens-Entscheidungen betrachten zu können, führen die Autoren die Variable *Gefahrenbewusstsein* (*threat awareness*) ein. Menschen, die sich der Gefahren bewusst sind, sind motiviert und in der Lage, die *Authentizität der Email* einzuschätzen und ziehen die *Eigenschaften des Senders* nur bei einem positiven Urteil zur weiteren Meinungsbildung heran (Pfeiffer et al., 2013). Menschen, die sich der Gefahren nicht bewusst sind, wissen nicht, dass Informationen bezüglich des Senders und Inhalts auch gefälscht sein können und vertrauen deshalb einer Email, wenn sie dem angeblichen Sender vertrauen (Pfeiffer et al., 2013). Das *Gefahrenbewusstsein* wird im Rahmen des Modells aus einer Kombination von Wissen und Erfahrung bezüglich der Bedrohung und dem potentiellen Umgang mit der Bedrohung geschlossen und wirkt sich an vielen Stellen als Moderator auf Zusammenhänge aus. Es wird zum Teil auch beeinflusst von dem *Kontext*, in dem die Nachricht erhalten wurde. Dieser setzt sich aus Faktoren wie der Plausibilität der Email und der wahrgenommenen Verwundbarkeit des verwendeten Computers gegenüber Angriffen zusammen und beeinflusst außerdem das Vertrauen in Sender, bzw. Nachricht, das wahrgenommene Risiko und den erwarteten Nutzen.
Die *Persönlichkeitseigenschaften des Empfängers*, bzw. der potentiell handelnden Person stellen eine weitere wichtige Gruppe von Variablen dar. Darin sind Faktoren, wie Neigung der Person anderen zu vertrauen, deren Neigung Risiken einzugehen und deren Ausmaß an Gehorsamkeit und Engagement, zusammengefasst. Diese beeinflussen das *wahrgenommene Risiko* und das *Vertrauen* in den Sender, bzw. die Nachricht. Die *demographischen Eigenschaften* der potentiell handelnden Person, wie Alter, Geschlecht und Bildung korrelieren sowohl mit dem *wahrgenommenen Risiko*, als auch mit dem *Gefahrenbewusstsein* (Pfeiffer et al., 2013).

2.4.2 Umgang mit Risiken im Kontext des Internets

In Kapitel 2.3 wurde bereits dargestellt, wie Nutzer sich und ihre Daten im Rahmen des Internetshoppings schützen können, bzw. wie sie sich sicher verhalten können. Nach Ergebnissen unterschiedlicher Studien scheinen sie das allerdings überwiegend nicht zu tun. So zeigt eine vom Bundesamt für Sicherheit in der Informationstechnik in Auftrag gegebene repräsentative Befragung von KANTAR TNS, dass nur ca. die Hälfte der Befragten sich sicher verhält (Bundesamt für Sicherheit in der Informationstechnik, 2017a). So achten immerhin 55,3% der Befragten auf eine verschlüsselte

Verbindung beim Onlineshopping und 43,6% nutzen dafür keine öffentlichen WLAN-Verbindungen. Bei der Einschätzung der Vertrauenswürdigkeit eines Online-Shops geben nur 48,6% der Befragten an, sich anhand der in Kapitel 2.3.3 beschriebenen Merkmale des Shops, wie z. B. einer vollständigen Anbieterkennzeichnung, vorhandener AGB oder Datenschutzbestimmungen zu orientieren. Acquisti und Grossklags (2005) stuften die Nutzung vorhandener Sicherheits-Technologien, wie beispielsweise die Verschlüsselung von Emails, durch 67% der Probanden, als eher niedrig ein.
Interessant ist, dass die Nutzer aber besorgt über den Umgang von Konzernen mit ihren persönlichen Daten sind (Raman & Pashupati, 2004; Tsai et al., 2011). So gaben in einer von Buxmann (2015) dargestellten Studie im Jahr 2012 62% und im Jahr 2014 75% der Befragten an, dass sie gegen eine kommerzielle Verwendung von Nutzerdaten sind. Auch in der Studie von Beresford, Kübler und Preibusch (2012) gaben 75% ein großes Interesse an Datenschutz und 95% ein Interesse am Schutz ihrer persönlichen Informationen an. Allerdings gaben nur ca. 14% der Befragten in der von Buxmann (2015) dargestellten Studie an, auf datenbasierte Dienste wie Facebook und Google zu verzichten.
Die widersprüchliche Beziehung zwischen der Intention ihre Daten zu schützen bzw. Daten preiszugeben und ihrem tatsächlichen Verhalten wird von Norberg et al. (2007) das Privacy Paradoxon genannt (siehe Kapitel 1.1). Begründungen, warum es zu dieser Widersprüchlichkeit kommt, gibt es verschiedene (Tsai et al., 2011). In manchen Fällen führten schon geringe Belohnungen dazu, dass die Befürchtungen zur Seite geschoben wurden (Acquisti & Grossklags, 2005). Schon die Aussicht auf nützliche Informationen führen dazu, dass Nutzer sich registrieren, um sie zu erlangen (Norberg et al., 2007). In der Studie von Beresford et al. (2012) brachte 1€ Preisnachlass den Großteil der Probanden dazu, ihre monatlichen Einkünfte und ihr Geburtsdatum preiszugeben. Neben eventuellen Begünstigungen ist der vermeintliche Aufwand, den der Schutz der persönlichen Daten den Nutzern abverlangt, immer wieder ein Argument. Der Aufwand ergibt sich aus der Beschaffung relevanter Informationen (Boos, 2015). Diese sind häufig schwer zu finden, was dazu führt, dass Nutzer sich selten die Mühe machen, danach zu suchen (Tsai et al., 2011). Ihnen fehlt dafür die Motivation (Cranor, 2008; West, 2008; Whalen & Inkpen, 2005). Dies lässt vermuten, dass Nutzer eventuell mehr für Datenschutz bezahlen würden, wenn ihnen die entsprechenden Informationen leichter zugänglich wären (Tsai et al., 2011). Häufig helfen allerdings auch gefundene Informationen den Nutzern nicht weiter (Whalen & Inkpen, 2005).
Laut West (2008) wägen Nutzer den notwendigen Aufwand gegen den wahrgenommenen Vorteil bezüglich des Datenschutzes, bzw. der Datensicherheit und die wahrgenommene Chance ab, dass sowieso nichts Schlimmes passieren wird. Laut Greenwald, Olthoff, Raskin und Ruch (2004) führt eine falsche Einschätzung des Risikos zu einem inakkuraten Kosten/Nutzen Urteil. LaRose, Rifon und Enbody (2008) gehen dagegen davon aus, dass Gewinne und Kosten, die jeweils mit sicherem bzw. unsicherem Verhalten zusammenhängen, verrechnet werden. Die Vorteile des sicheren Verhaltens sind dabei nicht immer offensichtlich, im Gegensatz zu dem Zeitaufwand, den es bringt. Die Belohnung dafür, dass Nutzer sich sicher verhalten, ist, dass eben nichts passiert (West, 2008). Das darf nicht dazu führen, dass die Kosten (der Aufwand) als Argument verwendet dafür werden, gar nichts zu tun (LaRose et al., 2008). Denn, wenn dann auch nichts passiert, kommt es zu einer rudimentären Form des Lernens, die dazu führt, dass die Nutzer weiterhin so vorgehen (Bravo-Lillo et al., 2011).
Zusätzlich sehen Nutzer häufig kein ernsthaftes Risiko (LaRose et al., 2008) oder gehen davon aus, dass ihnen „schon nichts geschehen wird“ (Greenwald et al., 2004; West, 2008). So konnte eine in Kapitel 2.2.2 bereits vorgestellte Studie von Bitkom (2017a) zeigen, dass die Bereitschaft, sich gegen finanzielle Schäden, die durch Cybercrime entstehen zu versichern, nur sehr gering ist. In Anbetracht der Tatsache, dass bereits 65% von Cybercrime betroffenen Befragten angaben, daraufhin nichts unternommen zu haben (Bitkom, 2017a), mag dies auch auf den Zweifel an der Effektivität eines Schutzes zurückzuführen sein, den LaRose et al. (2008) als zusätzlichen Grund für unsicheres Verhalten nennen.

Einen weiteren Grund für unsicheres Verhalten sieht Cranor (2008) darin, dass manche Nutzer nicht in der Lage sind, fundierte Sicherheitsentscheidungen zu treffen. Auch Anderson und Agarwal (2010) sehen in privaten Nutzern des Internets, die nicht wie im Arbeitsumfeld geschult oder durch technisches Personal unterstützt werden, eine signifikante Sicherheits-Schwachstelle. In der Studie von Acquisti und Grossklags (2005) zeigte sich, dass selbst in der Gruppe der technikaffinen und gebildeten Nutzer nur die wenigsten über Wissen bezüglich der Verwendung der gefragten technischen Unterstützungen verfügten. 44% der Teilnehmer konnten außerdem kein einziges Gesetz nennen oder beschreiben, welches Datenschutz zum Inhalt hat.
Whalen und Inkpen (2005) kommen zu dem Schluss, dass Datensicherheit sehr komplex, schwer zu verstehen und leicht falsch anzuwenden ist. Dabei können Nutzer noch mit den Risiken umgehen, mit denen sie vertraut sind, scheinen das aber nicht auf andere Risiken übertragen zu können (Downs et al., 2006). Die Überlastung in Bezug auf die Datenschutzverantwortung kann zu einem Ohnmachtsgefühl der Nutzer führen, welche sich in Resignation auswirkt (Wambach, 2017). Raman und Pashupati (2004) postulieren, dass sich die Strategien, die Nutzer im Umgang mit der Sicherheit ihrer persönlichen Daten entwickeln, in zwei Kategorien einteilen lassen: Vermeidungsstrategien, wie z. B. Risiken zu ignorieren oder das Internet nicht zu nutzen (Youn, 2009), und konfrontative Strategien, wie sich Wissen anzueignen und den Umgang mit der Technologie zu erlernen (Youn, 2009). So kamen Acquisti und Grossklags (2005) zu dem Schluss, dass 75% ihrer Probanden Maßnahmen zum Schutz ihrer persönlichen Daten ergriffen, wie einen Einkauf vor Eingabe der Daten abzubrechen oder falsche Daten anzugeben. Dabei sind die verwendeten Strategien vielfältig und individuell. Damit zeigen sie auf, dass diese eventuell spezifischer betrachtet werden müssen.

2.4.3 Studien zur Erfassung von Risikoverhalten

In einer bereits in Kapitel 1.1 dargestellten, umfassenden Metaanalyse von 150 Studien zum Eingehen von Risiken, teilten Byrnes et al. (1999) die gefundenen Methoden zur Erhebung des Risikoverhaltens in Gruppen ein. Die erste Gruppe bilden die Aufgaben, die eine hypothetische Auswahl (*hypothetical choice*) beinhalten. Diese zeichnet sich aus durch die Wahl einer von zwei hypothetischen Optionen oder der Angabe eines akzeptablen Risikolevels. Probanden wurden dabei nie gefragt, ob sie das Verhalten auch tatsächlich zeigen würden und mussten auch nicht die Konsequenzen ihrer Wahl erleben.
Bei der zweiten Gruppe wurde das Risikoverhalten direkt erfragt (*self-reported behavior*). In diesen Studien wurden die Probanden um Angaben, bezüglich der Häufigkeit gebeten, mit der sie ein gewisses Risikoverhalten zeigen oder in der Vergangenheit gezeigt haben.
Beobachtetes Verhalten stellt die Grundlage für die dritte Gruppe (*observed behavior*) dar. Dieses beobachtete Verhalten teilten Byrnes et al. (1999) in acht Gruppen ein. Bei drei der acht Gruppen konnten Punkte oder Geld gewonnen oder verloren werden, entweder durch raten, mit Hilfe bestimmter Fähigkeiten im Rahmen von physischen Spielen oder durch Glückspiel. Eine weitere Gruppe stellten Studien zum Thema Auto fahren dar. Abhängig davon, ob es sich dabei um eine Simulator Studie handelte, bestand hier teilweise ein tatsächliches physisches Risiko. Dasselbe galt auch für die Gruppe deren Inhalte physische Aktivitäten, wie z. B. auf einem Esel reiten, darstellten. In einer weiteren Gruppe bestand das riskante Verhalten darin, an einem Experiment teilnehmen zu wollen, bei dem die Probanden einer gewissen physischen oder psychologischen Gefahr ausgesetzt wären. Die Studien, bei denen die Probanden ein intellektuelles Risiko eingehen konnten bildeten eine weitere Gruppe. Hierbei wurden den Probanden Aufgaben mit unterschiedlichen Angaben der Schwierigkeit vorgegeben und sie

sollten sich ihre Schwierigkeitsstufe selbst aussuchen. In der letzten der achten Gruppe wurden die Studien gesammelt, die sich keiner der anderen Gruppen zuordnen ließen.
Wie bereits mehrfach erwähnt besteht in Bezug auf das Verhalten von Nutzern zum Schutz der personenbezogenen Daten ein Unterschied zwischen dem was sie, z. B. im Rahmen einer Erhebung sagen und dem, wie sie sich tatsächlich verhalten (siehe Kapitel 1.1, und 2.4.2). Auch Byrnes et al. (1999) gelangten im Rahmen der Metaanalyse zu der Erkenntnis, dass sich die Einschätzungen zu hypothetischen Szenarien und entsprechende Beobachtungen von Verhalten unterscheiden. Dem entspricht das Ergebnis von Amichai-Hamburger und Vinitzky (2010), die den Zusammenhang zwischen Persönlichkeitsfaktoren und der Nutzung von sozialen Netzwerken untersuchten. Dabei bauten sie ihre Studie auf der von Ross et al. (2009) auf, mit dem Unterschied, dass sie Selbstauskünfte der Probanden in ihrer Studie durch das objektive Kriterium der auf Facebook hochgeladenen Informationen ersetzten. Im Gegensatz zu Ross et al. (2009) konnten sie so einen starken Zusammenhang zwischen Persönlichkeit und Verhalten auf Facebook nachweisen.
Die Erfassung tatsächlichen Risikoverhaltens erweist sich allerdings nicht immer als so einfach, da Teilnehmer einer Untersuchung im Rahmen der Forschungsethik keinem tatsächlichem Risiko ausgesetzt sein dürfen (Döring & Bortz, 2016).
Aus diesem Grund liegt der Fokus im Rahmen dieses Kapitels auf Lösungen bezüglich der Erfassung von tatsächlichem Risikoverhalten im Rahmen des Datenschutzes im Internet. Im Folgenden sind einige entsprechende Studien, in der Reihenfolge ihrer Veröffentlichung, dargestellt.

Whalen und Inkpen (2005) führten eine Studie durch, bei der sie tatsächliches Verhalten mittels Blickbewegungsanalyse untersuchten. Die Probanden bekamen dabei unterschiedliche Aufgaben, wie in einem Account einloggen oder eine Kreditkarte verwenden. Ihnen wurden dafür Passwort und Kreditkartendaten zu Verfügung gestellt, die sie im Verlauf des Versuchs wie ihre eigenen behandeln sollten. Die 16 Probanden konnten sich dabei frei im Internet bewegen. Im Hintergrund wurden allerdings von den Teilnehmern unbemerkt Verbindungen zu bestimmten Seiten, wie Bankaccounts als künstliche Seiten mit Hilfe eines Labor proxy-servers dargestellt. Die Erhebung beinhaltete zwei Phasen. In der ersten erfüllten die Probanden die gestellten Aufgaben mit den zu Verfügung gestellten Daten, ohne dass ein spezieller Hinweis auf den Schutz der Daten erfolgte. Im zweiten Teil wurden die gleichen Aufgaben erfüllt, allerdings wurde zuvor instruiert, dass die Teilnehmer jegliche Handlung vornehmen sollten, die es braucht, um zu entscheiden, ob es sicher war, die Aufgabe zu vollenden. Eine unsichere Seite sollte im anschließenden Fragebogen angemerkt werden. In jedem Fall sollten die Daten aber angegeben werden. Zwischen den beiden Teilen des Experiments wurde per Fragebogen mit Hilfe einer Liste von möglichen Beweisen für Sicherheit erfasst, woran sich die Probanden normalerweise orientieren. Die gleiche Liste wurde zum Abschluss verwendet, um zu erfragen, wodurch sich die Teilnehmer in dieser Phase ein Bild bezüglich der Sicherheit gemacht hatten. Die Autoren konnten für keine der aufgerufenen Webseiten einen Nachweis dafür finden, dass im ersten Teil des Experiments auf Sicherheit (Security) geachtet wurde. Sie begründen das damit, dass es sich nicht um die tatsächlichen Daten der Probanden handelte und damit, dass die Erfüllung von Aufgaben im Labor dazu führt, dass der Fokus einzig auf der Aufgabenerfüllung liegt. Sie gehen deshalb davon aus, dass es ihnen nicht gelang, normales Verhalten abzubilden.

Wu, Miller und Garfinkel (2006), welche die Wirksamkeit unterschiedlicher Sicherheits-Werkzeugleisten und Sicherheitsindikatoren im Kontext von Phishing auch mit einem Fake-Account untersuchten, kamen zu dem Schluss, dass ihre Probanden versuchten, die ihnen zu Verfügung gestellten Daten wirklich zu schützen. Sie begründen das damit, dass jeder der Probanden wenigstens einmal etwas unternahm, was

man als Argwohn bzw. Misstrauen deuten kann. Dabei handelte es sich in 23 Fällen um ein nicht angewiesenes Verhindern von Cookies oder einem Ausloggen nach Beendigung der Aufgabe. In sieben Fällen meldeten die Probanden eine Täuschung oder versuchten gewissenhaft herauszufinden, ob eine Webseite seriös war. Es sei hierbei erwähnt, dass das Entdecken und Melden von Fake-Seiten die übergeordnete Aufgabe der Probanden darstellte.

Schechter et al. (2007) untersuchten als tatsächliches Verhalten, ob Bankkunden ihre persönlichen Daten angaben. Die Probanden sollten im Rahmen des Versuches fünf online Banking Aufgaben bearbeiten. Die ersten beiden Aufgaben dienten vordergründig dazu, dass sich die Probanden mit der Seite und dem Log-In Prozess vertraut machen konnten. Ziel der anderen drei Aufgaben war es, herauszufinden, wie die Teilnehmer auf unterschiedliche auffällige Hinweise auf einen Angriff reagieren. Die Hinweise waren, die Abwesenheit der https Anzeige auf der Log-In Seite der Bank, die Abwesenheit eines normalerweise verwendeten Bildes zur Authentifizierung der Seite und das Einblenden einer Warnseite. Auf die Abwesenheit des Bildes zur Authentifizierung wurden die teilnehmenden Bankkunden mit einer Notiz hingewiesen, die dieses mit Wartungsarbeiten begründete. Die Warnung ersetzte die gesamte Log-In Seite und wies auf ein Problem mit dem Sicherheitszertifikat der Webseite hin. Sie bot die beiden Optionen, die Seite zu schließen, mit dem Hinweis, dass dies empfohlen würde oder fortzufahren, mit dem Hinweis, dass dies nicht empfohlen würde. Die Ergebnisse zeigten, dass alle Probanden ihre Daten angaben, obwohl kein https einen Hinweis auf eine verschlüsselte Verbindung gab. Nur zwei hielten ihre Daten zurück in der Bedingung bei der das Bild zur Seiten-Authentifizierung nicht vorhanden war. Nur die offensiv präsentierte und formulierte Warnung hielt immerhin 27 Probanden (47%) von der Eingabe ihrer Daten ab. Interessanterweise untersuchten Schechter et al. (2007) darüber hinaus, ob es einen Einfluss hat, ob Probanden eine Rolle spielen, indem sie nicht ihre eigenen Daten verwendeten. Die Hälfte dieser Probanden wurden zusätzlich mit einer entsprechenden Instruktion bezüglich des Themas Datensicherheit sensibilisiert. Es zeigte sich, dass sich die Probanden, die ihre persönlichen Daten verwendeten, sicherer verhielten als die Probanden, die eine Rolle spielten. Das veranlasste die Forscher dazu darauf hinzuweisen, dass im Rahmen von Studien, wann immer es möglich ist, die Eingabe der persönlichen Daten dem Verwenden von fiktiven Daten vorzuziehen ist. Bezüglich der Sensibilisierung der Probanden in Bezug auf das Thema Datensicherheit ergaben sich keine signifikanten Ergebnisse. Schechter et al. (2007) nennen als Einschränkungen im Rahmen ihrer Studie, dass die Probanden sich weniger sicher verhalten haben könnten als in der echten Welt. Sie begründen dies mit der Erhebung im universitären Umfeld und der Einverständniserklärung in der betont wird, dass keine sensiblen Daten der Probanden aufgezeichnet werden. Außerdem vermuteten sie, dass die Aussicht auf die Versuchspersonenentschädigung von $25 die Teilnehmer trotz eventueller Bedenken dazu gebracht hat, die Aufgaben zu vollenden. Darüber hinaus gehen sie davon aus, dass die Probanden schlussfolgern konnten, dass der Fokus der Studie auf Datensicherheit lag. Zusätzlich ist die Möglichkeit gegeben, dass sich die Probanden sicherer verhielten, da sie wussten, dass sie beobachtet werden.

Norberg et al. (2007) erfassten die Intention Daten preiszugeben zwar nicht im Kontext des Internets, da es sich bei der Untersuchung aber um eine wesentliche in Bezug auf das Privacy Paradoxon handelt, wird sie an dieser Stelle trotzdem dargestellt. Zur Erfassung der Intention, persönliche Daten preiszugeben, verwendeten sie einen Fragebogen, den die Probanden, bei denen es sich um Studenten in einem Klassenraum handelte, per Hand ausfüllten. Das Szenario darin beschrieb eine Bank, die eine spezielle Kreditkarte für Studenten entwickelt, bei der ein Teil des umgesetzten Geldes in speziellen Gutschriften zurückgezahlt wird. Der entsprechende Student sei nun ausgewählt worden an der

Entwicklung teilzunehmen, wofür 20$ Aufwandentschädigung gezahlt werden. Die eigentliche Aufgabe bestand darin, aus einer Auswahl von 17 Arten von Daten, wie z. B. Name, Adresse, Alter, Hobbies usw. diejenigen anzukreuzen, die man bereit wäre preiszugeben. Zwölf Wochen später erschien ein vermeintlicher Bankangestellter und bot das entsprechende Produkt an. Die Studenten erhielten eine Broschüre zur Beantragung einer solchen Kreditkarte, in der dieselben 17 Datentypen auszufüllen waren. Es wurde darauf hingewiesen, dass Daten, die man nicht preisgeben wolle, unausgefüllt bleiben sollten, um zu vermeiden, dass auf Fake-Daten zurückgegriffen würde. Bei der Auswertung der Daten wurde die Summen angekreuzter Daten, die die Studenten also in beiden Fragebögen bereit waren auszufüllen, miteinander verglichen. Das Ergebnis zeigte, dass signifikant mehr Daten preisgegeben wurden, als im Vorfeld angegeben. Dieses Ergebnis konnten Norberg et al. (2007) auch in einer zweiten Studie nachweisen, bei der zwei unterschiedliche Szenarien (Bank vs. Pharmazieunternehmen) verwendet wurden. Die Forscher schränken ein, dass man mit der Generalisierung ihrer Ergebnisse vorsichtig sein sollte, da es sich bei ihrem Klassenraum-Setting um eine eher vertrauensvolle Situation handelte, so dass die Studenten ihre Daten einer geringeren Gefahr ausgesetzt sahen. Sie kommen aber trotzdem zu dem Schluss, dass mehr Forschungsaufwand in die Erhebung von tatsächlichem Verhalten investiert werden muss und dass im Bereich des Datenschutzes die Intention keinen akkuraten Prädiktor dessen darstellt.

Tsai et al. (2011) untersuchten, ob eine prominentere Darstellung von Informationen bezüglich des Datenschutzes von Webshops dazu führt, dass Nutzer diese in die Entscheidung, ob sie bei diesem Shop kaufen, einbeziehen. Darüber hinaus überprüften sie, ob Nutzer, die eher besorgt bezüglich des Schutzes ihrer Daten sind, bereit sind, mehr zu investieren, um bei einem Anbieter zu kaufen, der einen besseren Schutz der Daten anbietet. Dazu befragten sie die Teilnehmer im Rahmen einer ersten Studie nach ihren Bedenken und verschiedenen Produkten bezüglich derer sich die Bedenken unterscheiden könnten. Die Ergebnisse der Befragung nutzen die Autoren als Grundlage für ein anschließendes Onlineshopping Experiment, um das Kaufverhalten zu erheben, welches mit einem abschließenden Interview endete. Es zeigte sich im ersten Schritt, dass die meisten Probanden keine Bedenken hatten, Produkte wie Büromaterialien zu kaufen. Zögerlicher wurden die Teilnehmer bei Produkten, die persönliche Werte und mentale Zustände kommunizieren. Am meisten Vorbehalte zeigten sich bei Produkten, die mit gewalttätigem Verhalten in Verbindung gebracht werden. Auf Basis dieser Untersuchung wurden für das weitere Vorgehen die beiden Produkte Batterien und Sexspielzeug ausgewählt.
In Bezug auf das Onlineshopping Experiment wurde den Probanden die Aufgabe gestellt, eine neue Suchmaschine zu testen. Hierfür wurden in einem vorangehenden Screening Probanden ausgewählt, die überdurchschnittlich hohe Bedenken bezüglich Datensicherheit geäußert hatten. In einer von drei Bedingungen wurden den Teilnehmern im Rahmen der Suchmaschine Informationen zu den Datenschutzbedingungen dargeboten. Dies erfolgte im Rahmen einer Skala mit vier Kästchen, deren Anzahl von gefüllten Kästchen der Übereinstimmung der Präferenzen des jeweiligen Probanden mit den Datenschutzbestimmungen auf der jeweiligen Seite symbolisierte. Die Ergebnisse zeigten, dass Teilnehmer, die Informationen zu den Datenschutzkonditionen im Rahmen der Suchmaschine gezeigt bekamen eher bei den Webshops kauften, die höher eingestuft wurden. Dies galt sogar, wenn deren Preis höher war. Die Teilnehmer der Kontrollgruppen präferierten dagegen die Anbieter mit dem niedrigsten Preis. Interessant, wenn auch von den Autoren nicht weiter erwähnt, ist, dass die im vorangegangenen Fragebogen ermittelten unterschiedlich großen Bedenken bezüglich der Produkte wohl nicht durch höhere Ansprüche bezüglich des Datenschutzes erklären lassen. Man hätte demnach erwarten können, dass Datenschutz bei dem zu erwerbenden Sexspielzeug eine größere Rolle spielt als bei den Batterien. Augenscheinlich zeigt sich das in den Daten nicht. Im Gegenteil wurde das

Sexspielzeug in der Experimentalgruppe häufiger auf Seiten mit wenig oder niedrigem Datenschutzlevel gekauft, als die Batterien. Das spricht dafür, dass in die Einschätzungen der Bedenken bezüglich der Produkte auch weitere Bedenken eingeflossen sind. Die Autoren selbst schränkten ein, dass ihre Untersuchung im Carnegie Mellon Usable Privacy and Security (CUPS) Labor nicht der normalen Shopping Umgebung entspricht. Darüber hinaus stellen sie in Aussicht, dass die Preisunterschiede der Produkte, welche die Nutzer bereit waren in Kauf zu nehmen, nur sehr gering waren. Der prozentuale Unterschied übertragen auf teurere Produkte würde sich vermutlich nicht replizieren lassen.
Dem könnte man hinzufügen, dass auch ihre Stichprobe nur eingeschränkt aussagekräftig ist, denn hier wurden nur Probanden eingesetzt, die große Bedenken bezüglich des Datenschutzes äußerten. Die Autoren schreiben, dass bei ihnen entgegen anderer Studien gezeigt werden konnte, dass Menschen bereit sind, für Privacy zu bezahlen. Die Frage stellt sich, ob dies auch ohne die Einschränkung der Stichprobe darstellbar ist. Darüber hinaus wurden den Probanden die zu kaufenden Produkte vorgegeben. Eventuell kommen andere innere Prozesse zum Tragen, wenn es sich um Produkte handelt, welche die jeweilige Person tatsächlich und freiwillig kaufen möchte.

Auch Egelman et al. (2008), die in ihrer Studie versuchten, möglichst realistische Szenarien zu schaffen, indem die Probanden für Online-Käufe im Rahmen des Experiments ihren persönlichen Email-Account und die eigene Bandverbindung nutzen mussten, erwähnen diesen Punkt. Sie gehen allerdings davon aus, dass der Einfluss ausgeglichen wird durch den Willen der Probanden, die Studie zu absolvieren. Sie befürchteten im Vorfeld, dass die Nutzer, sollten Sie sich selbst für Produkte entscheiden können, zu lange dafür brauchen würden und darüber hinaus andere Faktoren zum Tragen kämen, welche die Ergebnisse konfundieren könnten. Zusätzlich war das Ziel, dass die Probanden möglichst billige Produkte kaufen sollten, was im Rahmen der Aufwandsentschädigungen die Möglichkeit für zwei Käufe und zusätzliches Geld für die Teilnahme geben sollte. Die Probanden wurden deshalb aufgefordert eine Box Büroklammern für ca. 0.50$ und ca. 6$ Versand bei Amazon, bzw. ein Produkt ihrer Wahl bei einem günstigen chinesischen Elektronikmarkt, der Produkte im Bereich von 5-10$ anbot, via eBay zu kaufen. Den Probanden wurde eine Aufwandsentschädigung von 35$ gezahlt zusätzlich zu dem Preis, den sie für die beiden Käufe mit ihrer Kreditkarte bezahlten. Egelman et al. (2008) gehen dabei nicht davon aus, dass der Preis der Produkte eine Rolle spielt, da mögliche Angreifer bei Zugriff auf die Kreditkarte auch teurere Einkäufe tätigen könnten. Die Aufmachung als eine Studie zum Onlineshopping diente dabei nur zu Tarnung, um Verhalten in Bezug auf Warnungen im Kontext von Phishing zu untersuchen. Auf die Ergebnisse der Studie wird deshalb in diesem Rahmen nicht weiter eingegangen.

Auch Beresford et al. (2012) untersuchten die Bereitschaft ihrer Probanden für eine höhere Sicherheit ihrer Daten zu bezahlen. Dazu sollten die Teilnehmer eine DVD bei einer von zwei fiktiven Filialen eines existierenden Webshops erwerben, der seine Waren über Amazon verkauft. Von diesen beiden Filialen wurden unterschiedliche Daten der Kunden gefordert. Neben dem vollständigen Namen, der postalischen Adresse und der Emailadresse, die von beiden Shops erfragt wurden, war es bei einem der Shops notwendig das Geburtsdatum und das monatliche Einkommen anzugeben. Der andere Shop forderte stattdessen die Angabe des Geburtsjahres und der Lieblingsfarbe. In der einen Versuchsbedingung unterschieden sich die beiden Shops nur diesbezüglich. In der anderen Bedingung lagen die Preise des Shops, der eine Angabe bezüglich des monatlichen Einkommens forderte jeweils um einen Euro unter denen des Shops, bei dem stattdessen die Lieblingsfarbe angegeben werden musste. Die Ergebnisse zeigten, dass sich die Käufe bei gleichem Preis ungefähr gleich auf beide Shops verteilten. In der zweiten Bedingung zeigte sich, dass dem überwiegenden Teil der Probanden (39 von 42) das Vermeiden der Angabe ihres Einkommens nicht den zusätzlichen Euro wert war. Ein abschließender

Fragebogen bestätigte zum einen, dass sich die Probanden über den Unterschied der geforderten Daten bewusst waren und auch ihr Einkommen weniger gerne angeben wollten als ihre Lieblingsfarbe. Hier offenbaren sich Dissonanzen zwischen erfragten Einschätzungen und tatsächlichem Verhalten. Die Autoren bieten zwei Erklärungsmöglichkeiten dazu an. Entweder müssen sie ihre Fragebogendaten als nicht informativ ansehen, da sie nicht mit der tatsächlichen Auswahl übereinstimmen oder das gezeigte Verhalten widerspricht der sogenannten Theorie der offenbarten Präferenzen. Diese basiert auf der Idee, dass sich die Vorlieben von Konsumenten in ihrem Kaufverhalten offenbaren (Chambers & Echenique, 2016).
Insgesamt brachte die Studie also sehr interessante Ergebnisse, jedoch unterliegt auch sie einigen Einschränkungen. Die Autoren erwähnen selbst, dass die Stichprobe, die überwiegend aus Studenten bestand, einen Einfluss auf die Ergebnisse gehabt haben kann. Laut Döring & Bortz (2016) sehen Schülerinnen und Schüler Fragen nach dem Einkommen weit weniger kritisch als das Berufstätige tun. Diese Einschränkung versuchen Beresford et al. (2012) mit dem abschließenden Fragebogen abzufangen, in denen die Probanden ihre tatsächlichen Bedenken zum Ausdruck bringen. Positiv zu erwähnen ist außerdem, dass die Probanden echte Käufe mit ihren tatsächlichen Daten tätigten. Aus den Instruktionen ging hervor, dass die Daten tatsächlich an den verwendeten Shop und an Amazon übermittelt würden. Hierzu sei erwähnt, dass ein Anteil von 45.8% vom Umsatz, im Deutschen Online-Handel, den Amazon 2017 erzielen konnte (ECC Köln, 2018), dafür spricht, dass dieser Anbieter bei online Käufern tendenziell großes Vertrauen genießt.

2.4.3.1 Verwendete Messgrößen für Risikoverhalten im Kontext des Datenschutzes

Zur Operationalisierung des Risikoverhaltens im Kontext des Datenschutzes verwenden die dargestellten Studien unterschiedliche Messgrößen. Während die Einordnung des Verhaltens bei Wu et al. (2006) auf Beobachtungen des Verhaltens während der Bearbeitung einer bzw. mehrerer Aufgaben basiert, verwenden andere die Art und/oder die Anzahl preisgegebener Daten als Maß (siehe Amichai-Hamburger & Vinitzky, 2010; Norberg et al., 2007). Auch das dichotome Maß, ob Daten angegeben wurden oder nicht (Schechter et al., 2007) oder bei welchem von unterschiedlichen Webshops der geforderte Einkauf getätigt wurde (Tsai et al., 2011), wird als Messgröße bezüglich des Risikoverhaltens verwendet.
Während sich bei Letzteren die Ausprägungen des erfassten Verhaltens auf zwei Möglichkeiten beschränken, kann bei den davor beschriebenen Verfahren das Verhalten differenzierter beschrieben werden. Dabei bezieht sich die Überprüfung von Art und Anzahl preisgegebener Daten eher auf das Ergebnis, welches sich aus einem bestimmten Verhalten ergibt. Hierbei ist es möglich, dass unterschiedliches Verhalten zu gleichen Ergebnissen führt. Die differenzierteste Untersuchung gezeigten Verhaltens ist demnach mit Hilfe der Verhaltensbeobachtung möglich. Aus dem Grund ist diese Methode im Rahmen psychologischer Untersuchungen von großer Bedeutung (Huber, 2005). Dabei kann die direkte Beobachtung, die mit dem „bloßen Auge“ erfasst und per schriftlicher Protokolle oder Videoaufnahmen festgehalten wird (Zimbardo & Gerrig, 2003), unterschiedlichen Beobachtungsfehlern, wie z. B. Urteilsverzerrungen durch Erwartungshaltungen unterliegen (Döring & Bortz, 2016; Endruweit, 2014). Demgegenüber steht die häufig präzisere, sogenannte indirekte Beobachtung, für die allerdings entsprechende Ausrüstung und Instrumente zur Verfügung stehen muss (Zimbardo & Gerrig, 2003). Whalen und Inkpen (2005) verwendeten im Rahmen ihrer Studie die sogenannte Blickbewegungsanalyse. Dabei werden die Bewegungen der Augen der Probanden erfasst. Diese können dann auf Projekte in der Umgebung, oder in dem Fall auf dem Bildschirm bezogen werden. Der Vorteil

hierbei ist, dass es sich dabei um eine willentlich schwer zu beeinflussende und objektive Messgröße handelt.

Fazit

Zur Erklärung menschlichen Risikoverhaltens werden die unterschiedlichsten Theorien und Modelle herangezogen. Einige stellen dabei generelle Zusammenhänge dar, andere, hier dargestellte, sind auf Verhalten in Bezug auf ein Risiko angepasst. Die ältesten dieser Theorien behandeln vorwiegend Risiko im monetären Kontext, welches über Gewinn bzw. Verlust definiert wird. Theorien, die sich aus diesen vergleichsweise berechenbaren Kontext lösen, verwenden Einflussfaktoren, die sich auf die Einschätzung des jeweiligen Risikos, dargestellt durch Auftretenswahrscheinlichkeit, Erwartung oder Risiko vs. Nutzen-Verrechnungen beziehen. Diese Einschätzung eines Risikos unterscheidet sich abhängig von unterschiedlichen Charakteristika der jeweiligen Personen und dem jeweiligen Kontext. Allen Modellen gemeinsam ist die Problematik, dass tatsächliches Verhalten unter Risiko schwer erhoben werden kann, ohne teilnehmende Probanden einem tatsächlichen Risiko auszusetzen. Meist wird deshalb von der vorangehenden Intention auf das Verhalten geschlossen. In Bezug auf Datenschutz-Verhalten scheint dieses Vorgehen allerdings weniger geeignet, wie Untersuchungen bezüglich des tatsächlichen Umgangs der Menschen mit Risiken im Kontext des Internets zeigen. Obwohl sie danach gefragt häufig anderes aussagen, schützen viele Menschen ihre Daten im Internet nur wenig. Fehlende Motivation dem hohen Aufwand der Informationssuche zu begegnen, fehlende Kenntnisse und Resignation aufgrund von Überforderung werden hier unter anderem als Gründe genannt. Um die teilweise schlechte Passung zwischen Aussagen von Probanden und dem tatsächlichen Verhalten zu umgehen, versuchen einige Forscher möglichst realistische Szenarien zu schaffen, welche die Erfassung tatsächlichen Verhaltens ermöglicht. Sie unterliegen dabei allerdings trotz allem unterschiedlichen Einschränkungen wie einer eingeschränkten Stichprobenzusammensetzung oder der Nutzung von Fake-Accounts. Auch nutzen sie unterschiedliche Messgrößen um Risikoverhalten im Kontext des Datenschutzes zu beschreiben. Die sogenannte Blickbewegungsanalyse wird dabei als besonders vielversprechend in diesem Kontext angesehen. Aus dem Grund beschäftigt sich das folgende Kapitel mit der Beschreibung dieser Methodik.

2.5 Erfassung von Verhalten mittels Blickbewegungsanalyse

Die Bewegungen der Augen werden als objektives Maß angesehen, welches die Untersuchung vieler biologischer und psychologischer Prozesse, wie z. B. das Sehen oder die Wahrnehmung ermöglicht (Wade & Tatler, 2005). Da die Erfassung von Verhalten mittels Blickbewegungsanalyse als Möglichkeit in Betracht gezogen wird, auch tatsächliches Verhalten zum Schutz der eigenen Daten im Rahmen von Onlineshopping abbilden zu können, wird diese Methode im folgenden Kapitel eingehender betrachtet.

2.5.1 Geschichte der Blickbewegungsanalyse

Analysen der Blickbewegungen bildeten schon früh die Basis für Forschungen bezüglich des Lesens oder Aspekten des visuellen Gedächtnisses (Wade & Tatler, 2005). Die älteste angewendete Technik dabei ist die direkte Beobachtung der Augen. Einschränkungen stellen dabei allerdings die Geschwindigkeit und die Auflösung der zu beobachtenden und der beobachtenden Augen, sowie die Subjektivität der Daten dar (Wade & Tatler, 2005).

Laut Holmqvist et al. (2011) wurden die ersten Eye-Tracker Ende des 19. Jahrhunderts hergestellt. Die Forschung damit war sehr aufwändig und oft invasiv. So verwendete Huey (1898) eine selbst erfundene mechanische Vorrichtung, die mit Hilfe eines Hebelarms die Bewegungen der Augen auf eine Oberfläche übersetzte (Wade & Tatler, 2005). Um mit Hilfe dieses Apparates Blickbewegungen aufzeichnen zu können, mussten die Köpfe der Probanden mittels eines Mundstückes mit dem Zahnabdruck in Wachs fixiert werden. Zwinkern der Augenlider wurde durch eine Vorrichtung verhindert und ein kleines Schälchen aus Gips auf der Hornhaut befestigt. Dafür wurde das Auge im Vorfeld mittels Kokain anästhesiert. Delabarre (1898), dessen Beitrag zur Forschung in eben diesem Gipsschälchen lag, schloss durch die Methode bedingte eventuelle Schädigungen des jeweiligen Auges dadurch aus, dass die unangenehmen Effekte bald verschwunden waren und er ein Jahr später keine negativen Auswirkungen mehr feststellen konnte.
Diese frühen und ausschließlich mechanischen Untersuchungen der Augenbewegungen waren darüber hinaus eingeschränkt durch das Fehlen einer messbaren zeitlichen Komponente des Sehens (Dodge & Cline, 1901). Diese Lücke schlossen Dodge & Cline (1901) ein paar Jahre später mit Hilfe der Photographie. Neben Reflektionen, die damals bereits häufig verwendete, verschiedenen Arten von Kontaktlinsen hervorbrachten, fotografierten sie außerdem die Reflektionen, die sich auf der Oberfläche des Auges selbst ergaben (Wade & Tatler, 2005). Die dafür notwendigen optischen Geräte bilden die Grundlage der meisten heute erhältlichen Eye-Tracker (Wade & Tatler, 2005). Rayner (1998) sieht bis zum Jahr 1920 die erste Ära der Erforschung der Augenbewegung. Sie brachte viele Grundlagen hervor wie die Erkenntnis, dass während der Bewegung der Augen keine Informationen aufgenommen werden oder wie groß der Bereich des effektiven Sehens ist (Rayner, 1998).
In den darauffolgenden Jahren wurden die Techniken, um Blicke von Probanden aufzuzeichnen, immer weiterentwickelt und verfeinert. Weitere Schritte in der Entwicklung stellten 1935 die Nutzung von photoelektrischen statt photographischen Aufnahmemedien von Dohlman und die Verwendung von Infrarot anstatt sichtbarem Licht dar (Wade & Tatler, 2005). Zu einem weiteren großen Fortschritt führte 1948 die Entwicklung des ersten head-mounted Eye-Trackers von Hartridge und Thompson, die freie Kopfbewegungen der Probanden ermöglichte (Jacob & Karn, 2003).
Bis in die 70er Jahre des 20. Jahrhunderts lag die Entwicklung der entsprechenden Techniken und Apparaturen dabei allein in der Hand der Wissenschaftler, die sie anwendeten. Diese Tatsache machte die Blickbewegungsanalyse sehr aufwändig, exklusiv und unpraktisch, hatte aber den Vorteil, dass die Anwender sich mit dem jeweiligen System, dem Umgang damit und den resultierenden Daten bestens auskannten (Holmqvist et al., 2011). Eventuell trug die notwendige Spezialisierung jedoch dazu bei, dass Rayner (1998) diese von ihm als zweite Ära benannte Zeit als eher stagnierend beschreibt. Er beruft sich dabei auf eine Zusammenfassung aktueller Studien von Tinker (1958), der zwar die technischen Fortschritte in Bezug auf die Erfassung der Blickbewegungen anerkennt, der aber inhaltlich bemängelt, dass man nach Durchsicht der weniger werdenden Literatur zu dem Schluss kommen könnte, dass es kaum weitere Erkenntnisse geben kann. Er bezieht sich dabei auf die Untersuchungen der Augen beim Lesen. Möglicherweise führte dieser Eindruck dazu, dass es zwischen den späten 1950er Jahren bis in die 1970er Jahre nur wenig Forschung zu Augenbewegung gab (Rayner, 1998). Das änderte sich in den folgenden Jahren dadurch, dass kommerziell, von Ingenieuren entwickelte Produkte auf den Markt kamen. Laut Rayner (1998) zeichnet sich die dritte Ära durch Verbesserungen der Aufnahme-Systeme aus, welche die Messungen genauer und einfacher machten. Ein besonders großer Fortschritt war dabei die Möglichkeit das Eye-Tracking System mit einem Computer verbinden zu können. Dadurch konnte eine viel größere Menge Daten erhoben und analysiert werden (Rayner, 1998). In den 1990er Jahren stieg die Popularität der Blickbewegungsanalyse wieder an (Salvucci & Goldberg, 2000). Den Beginn einer vierten Ära sieht Duchowski (2002) in der Entstehung von interaktiven Anwendungen mittels

Blickbewegung. Durch die Fortschritte im Bereich der Fähigkeiten von Computern, kann der Eye-Tracker heute als Eingabegerät in verschiedenen Anwendungen fungieren (Duchowski, 2002). Eines der ersten auf Blickbewegungsanalyse basierenden interaktiven Systeme stellte Jacob (1990) vor. Im Gegensatz zu vorangegangenen Ansätzen bei denen die Interaktion von den Probanden zunächst gelernt werden musste, konnte mit seinem System der Eindruck erweckt werden, dass das System auf die Intention des Nutzers reagiert.
Die heutige Zeit zeichnet sich durch eine steigende Verfügbarkeit aus (Holmqvist et al., 2011). Blickbewegungsanalyse wird in vielen Disziplinen und Bereichen eingesetzt. Beispiele hierfür sind die Usability Forschung, die kognitive Psychologie, die Psycholinguistik, die Sportwissenschaften, Neurophysiologie (Holmqvist et al., 2011), aber auch Informatik, Wirtschaftsingenieurwesen und Marketing (Duchowski, 2002). Darüber hinaus wird sie auch im Rahmen von Arbeitsplatzgestaltung, z. B. im Cockpit oder Fahrzeug verwendet (Heidmann & Ziegler, 2002). Eine moderne Variante der optischen Eye-Tracker, bei denen sich bislang das Aufnahmegerät und die Lichtquelle sehr nah am Auge befanden, stellt der sogenannte Remote Eye-Tracker dar (Wade & Tatler, 2005). Hierbei befindet sich das Aufnahmegerät vor den Probanden. Die Tatsache, dass sich nun deren Kopf freier bewegen konnte führte zu noch breiteren Anwendungsmöglichkeiten, wie Studien mit Kindern, über Mensch-Computer Interaktion oder zur Fahrzeugführung (Wade & Tatler, 2005).

2.5.2 Bilderfassung

Generell lassen sich die Operationen im Rahmen einer Blickbewegungsanalyse in die Bereiche Bilderfassung, Bildanalyse und Blickbewertung einteilen (Holmqvist et al., 2011). Um verstehen zu können, wie Bilderfassung funktioniert, ist es notwendig, einige Grundlagen bezüglich des Aufbaus der Augen und des Vorgangs des Sehens zu kennen. Dieser beginnt mit einem Objekt in unserer Umwelt, das Licht reflektiert, welches vom Auge aufgenommen wird (Goldstein, 2008). Dort wird das Licht mittels Rezeptoren in elektrische Signale umgewandelt, die zum Gehirn weitergeleitet werden (Goldstein, 2008). Abbildung 5 zeigt diesen Vorgang und den Aufbau des Auges.

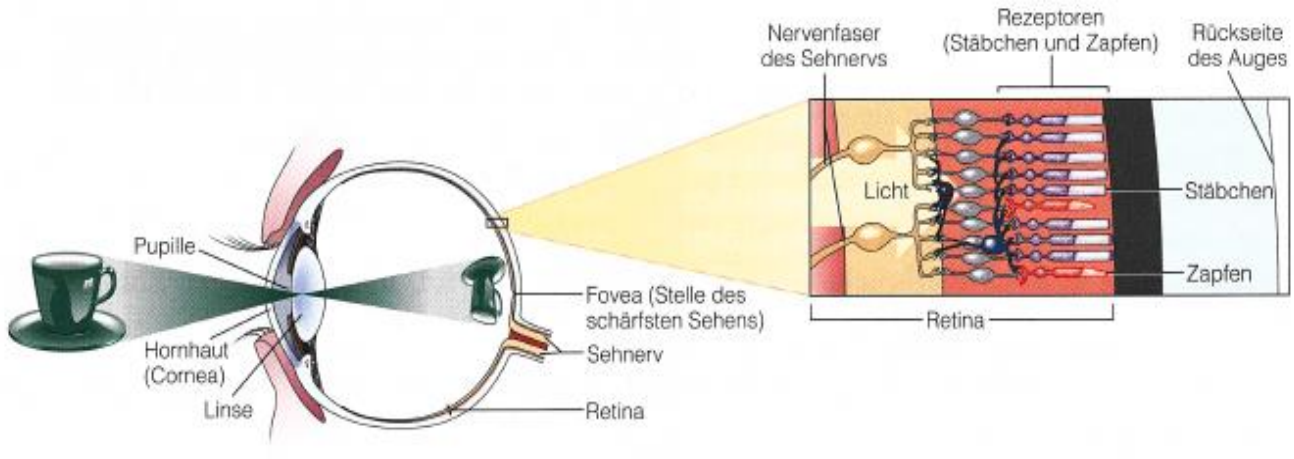


Abbildung 5. Darstellung der visuellen Informationsaufnahme und der Reizweiterleitung aus Goldstein (2008, S. 30).

Das Licht tritt durch die Pupille in das Auge ein und wird umgekehrt auf der Retina abgebildet (Schlick, Bruder & Luczak, 2018). Dort existieren zwei unterschiedliche Arten visueller Rezeptoren, Zapfen und Stäbchen, die wiederum unterschiedliche Aufgaben erfüllen (Goldstein, 2008; Schlick et al., 2018). Während die Zapfen bezüglich Details und Farbe empfindlich sind, gilt das bei Stäbchen für Helligkeit (Holmqvist et al., 2011). Beide leiten die Informationen weiter über den Sehnerv an das Gehirn. Zapfen und Stäbchen sind auf der Retina nicht gleich verteilt (Schlick et al., 2018). So existieren auf einem kleinen Teil ausschließlich Zapfen. In diesem Fovea genannten Areal, welches sich über weniger als 2° des visuellen Feldes erstreckt, wird die höchste visuelle Qualität erreicht (Helo, Pannasch, Sirri & Rämä, 2014; Holmqvist et al., 2011). Um Objekte in unserer Umgebung scharf sehen zu können, müssen wir unsere Augen demnach schnell so bewegen, dass das Bild des anvisierten Objektes in der fovealen Region liegt (Helo et al., 2014). Die Position der Pupille wird deshalb verwendet, um eine Aussage darüber machen zu können, wohin das Auge schaut. Heutige Eye-Tracker ziehen zur Bestimmung der Position der Pupille ein Kamerabild des Auges heran (Holmqvist et al., 2011). Mittels unterschiedlicher Bilderkennungsalgorithmen erkennt das System darauf die Position der Pupille. Um deren Bewegungen erfassen zu können, benötigt der Eye-Tracker einen zweiten Punkt als Referenz. Dafür wird ein Infrarotlicht auf das Auge gerichtet, welches zu einer Reflektion auf der transparenten Hornhaut auf der Vorderseite des Auges (Goldstein, 2008), der Cornea, führt. Die relative Distanz zwischen der Position der Pupille und der cornealen Reflektion nutzt das System, um die Blickposition zu berechnen (Holmqvist et al., 2011). Um diese einem bestimmten Stimulus zuordnen zu können, bedarf es einer Kalibrierung. Typischerweise werden dem Probanden dafür 2, 5, 9, 13 oder 16 Punkte angezeigt, auf die nacheinander geschaut werden soll (Holmqvist et al., 2011). Zusätzliche Angaben wie die genaue Größe und Position der Kalibrierungspunkte sowie den Abstand des Auges zum Monitor, auf dem diese Punkte präsentiert werden, werden manuell vorgegeben oder vom System geschätzt bzw. gemessen. Zusammen mit den Positionsangaben der Pupille und der cornealen Reflektion ist es dem System mit Hilfe der Geometrie möglich, eine Funktion aufzustellen, die auf Basis der aktuellen Position von Pupille und cornealer Reflektion die Position des jeweiligen Stimulus abschätzen kann, auf den gerade geschaut wird (Holmqvist et al., 2011). Die Verwendung einer zweiten Infrarotquelle bringt dabei zusätzliche Stabilität. Insbesondere bei Kopfbewegungen, verkompliziert dies aber das mathematische Modell zusätzlich (Holmqvist et al., 2011). Probleme, die bei der Datenerfassung auftreten können, sind bei Holmqvist et al. (2011) beschrieben. So können die Pupille oder die Reflektion verdeckt werden. Dies kann z. B. durch schlaffe Augenlider oder Lachen der Fall sein. Auch kann z. B. Mascara, eine Brille, feuchte Augen oder auch umgebenes Sonnenlicht dazu führen, dass die Pupille und die corneale Reflektion teilweise oder gar nicht erkannt werden.

Um Blicke ohne Unterbrechungen nachverfolgen zu können, muss diese Position häufig gemessen werden. Die Häufigkeit, in der das geschieht, wird Abtastrate genannt und in Hz angegeben (Holmqvist et al., 2011). Ein Eye-Tracker mit 50 Hz Abtastrate nimmt die Blickrichtung 50 mal pro Sekunde auf (Holmqvist et al., 2011). Je niedriger die Abtastrate, desto mehr Zeit verstreicht zwischen zwei Positionsberechnungen, in der Bewegungen nicht aufgezeichnet werden. Die Fehler in der Schätzung des Blickverlaufes sinken demnach bei steigender Abtastrate. Die Grenze ab der nicht mehr von einem Niedrig-, sondern von einem Hochgeschwindigkeitssystem gesprochen wird, liegt bei 250 Hz (Holmqvist et al., 2011). Diese Geräte sind dann entsprechend teurer und produzieren ein entsprechend größeres Datenvolumen (Holmqvist et al., 2011). Je nach dem, was untersucht werden soll, kann eine niedrigere Abtastrate aber auch ausreichen (Jacob & Karn, 2003).

2.5.3 Bildanalyse

Für die Bildanalyse und die anschließende Blickbewertung liefert der Eye-Tracker zunächst ganz grundlegende Daten. Diese sind die Position des Blickes (in x- und y-Koordinaten), die Geschwindigkeit der Augenbewegung (in °/s) sowie die Beschleunigung der Augenbewegung (in °/s²) (Holmqvist et al., 2011). Eine weniger häufig verwendete Größe stellt der Pupillendurchmesser dar. Aus diesen Daten können implementierte Algorithmen im nächsten Schritt definierte Ereignisse herausfiltern. Wie bereits erwähnt, bewegen sich die Augen während des Sehens immer so, dass Objekte, die genauer betrachtet werden, auf der Fovea abgebildet werden können. Eine solche Pause über einer informativen Region von Interesse wird Fixation genannt (Salvucci & Goldberg, 2000). Zwischen den Fixationen bewegen sich die Augen schnell zur nächsten Fixation (Sibert & Jacob, 2000). Diese Bewegung wird Sakkade genannt (Loftus & Mackworth, 1978) und entsteht aus der schnellsten Bewegung, zu der der menschliche Körper fähig ist (bis 700°/s) (Schlick et al., 2018). Zwar machen die Augen zusätzlich sehr schnelle minimale Bewegungen, diese werden aber vom Sehenden nicht realisiert (Sibert & Jacob, 2000). Fixationen und Sakkaden stellen die generellen Mechanismen im Rahmen des Sehens dar (Sibert & Jacob, 2000). Die Informationsaufnahme findet dabei fast ausschließlich während der relativ stabilen Fixationen statt (Helo et al., 2014). Während der Sakkaden ist diese unterdrückt (Holmqvist et al., 2011; Rayner, 1998; Sibert & Jacob, 2000). Diese Tatsache scheint sich sowohl in Einschränkungen der Reaktionszeiten der Photorezeptoren, als auch in aktiver Unterdrückung des visuellen Verarbeitungsweges während dieser Bewegungen zu begründen (Wade & Tatler, 2005). Fixationen werden dagegen mit intensiver kognitiver Verarbeitung in Verbindung gebracht (Pan et al., 2004). So gilt die Dauer der Fixation als Maß für die kognitive Verarbeitungstiefe (Velichkovsky, Sprenger & Pomplun, 1997). Die Weite der Pupille gibt darüber hinaus einen Hinweis auf das individuelle Interesse oder den Grad der Erregung bezüglich des Gesehenen (Granka, Joachims & Gay, 2004).
Um diese aussagekräftigen Ereignisse im Rahmen der Blickverläufe identifizieren zu können, greifen die verwendeten Algorithmen auf unterschiedliche Maße zurück. Manche stützen ihre Auswertung dabei auf räumliche Kriterien wie Geschwindigkeit, Streuung oder Interessensgebiet (*area of interest*), andere verwenden zeitliche Kriterien wie Dauer oder lokale Anpassung (*local adaptivity*) (Salvucci & Goldberg, 2000). Bei der Verwendung von Geschwindigkeiten und Beschleunigungen als Grundlage bedarf es einer höheren Abtastrate (>200Hz) (Holmqvist et al., 2011). Neben der Verwendung eines entsprechenden Algorithmus ist es auch möglich, die Ereignisse per Hand zu detektieren (Holmqvist et al., 2011). Ziel der Identifikation aussagekräftiger Ereignisse ist die Reduktion der Komplexität der vorliegenden Daten, ohne dabei die essentiellen Charakteristika zu verlieren oder zu verfälschen, die Aufschluss über Kognition und visuelle Verarbeitung liefern sollen (Salvucci & Goldberg, 2000). Dieser Prozess stellt deshalb einen wesentlichen Teil der Blickbewegungsanalyse dar, der große Auswirkungen auf übergeordnete Analysen haben kann (Salvucci & Goldberg, 2000).
Probleme bezüglich der Identifikation der Ereignisse liegen aber häufig nicht an fehlender Fähigkeit zu Präzision oder Flexibilität der Algorithmen (Salvucci & Goldberg, 2000), sondern in einer eindeutigen für alle geltenden Definition. Darüber, wie genau eine Fixation zu beschreiben ist, ist man sich in der Literatur nicht gänzlich einig. Laut Holmqvist et al. (2011) werden Fixationen meist durch ein Kriterium der maximal erlaubten Streuung oder Geschwindigkeit ermittelt. Die Autoren stellen dar, dass im ersten Fall zeitlich nebeneinanderliegende Samples (Proben) für eine minimale Dauer („laut Literatur irgendwo zwischen 50-250 ms“) innerhalb einer räumlich begrenzten Region liegen (typischerweise 0.5-2.0°) müssen. Im zweiten Fall sind Fixationen definiert als örtlich benachbarte Anteile der Blickdaten, bei denen die Blickgeschwindigkeit eine gewisse Grenze (10-50°/s) nicht übersteigt (Holmqvist et al., 2011). Salvucci und Goldberg (2000) geben einen Überblick über verschiedene Algorithmen, die verwendet

werden können, um Fixationen und Sakkaden zu identifizieren. Für die Algorithmen, deren Erkennung auf Geschwindigkeitsunterschieden basieren, geben sie eine Geschwindigkeit von <100°/s als Definition für Fixationen an. Laut ihnen liegt die Grenze bezüglich der Streuung bei 0,5-1° des Sehwinkels, wenn die Entfernung des Auges zum Stimulus bekannt ist. Als zeitliche Grenze schlagen sie einen Wert für das Verharren des Blickes zwischen 110-200 ms vor. Zusätzlich geben sie an, dass Fixationen selten kürzer als 100ms sind und oft im Bereich von 200-400 ms liegen. Laut Granka et al. (2004) sind Fixationen definiert als räumlich stabile Blicke, die ungefähr 200-300 ms dauern, während denen die visuelle Aufmerksamkeit auf ein bestimmtes Areal des visuellen Feldes gerichtet ist. Jacob & Karn (2003) beschreiben Fixation als eine relativ stabile Position der Augen im Kopf mit einer maximalen Streuung von typischerweise ∼2°, mit einer minimalen Dauer (typischerweise 100-200 ms) und mit einer Geschwindigkeit unter normalerweise 15-100°/s. Für den von Sibert & Jacob (2000) verwendeten Algorithmus wurden Augenpositionen, die sich für mindestens 100 ms innerhalb von 0,5° bewegten als Fixationen beschrieben. Sie gaben außerdem die Dauer von Fixationen mit 200-600 ms an. Auch Taylor et al. (2015) beschreiben Fixationen sehr genau. Laut ihnen sind das konsistente Augenpositionen, die sich innerhalb von 2° des Sehwinkels mit einer minimalen Dauer (normalerweise 100-200 ms) und einer Geschwindigkeit bewegen, die unter 15-100°/s liegt. Sie verwenden allerdings in der eigenen Studie die Grenzen von mindestens 120 ms in einem Bereich von ungefähr 1 cm. Bei anderen Forschern bezieht sich die Beschreibung von Fixationen ausschließlich auf die eigene Studie. So geben Pan et al. (2004) eine Fixation als eine Serie von 3 oder mehr Messungen an, die sich für mindestens 200 ms in einem Radius von 40 Pixeln bewegen. Bei Ollerman (2004) wird die maximale räumliche Ausdehnung dagegen mit 12 pt und eine minimale Dauer von 100 ms angegeben.

Häufig werden in der Literatur auch Angaben gemacht, die sich ausschließlich auf die Dauer der Blickzuwendung beschränken. Diese liegen zum Beispiel bei 200-300 ms (Rayner, 1998), 200-400 ms (Goldberg, Stimson, Lewenstein, Scott & Wichansky, 2002) oder ca. 300 ms (Loftus & Mackworth, 1978; Wade & Tatler, 2005) . Genauer sind Fixationsdauern dagegen bei Poole & Ball (2006) angegeben. Laut ihnen dauern Fixationen im Durchschnitt 218 ms in einem Bereich von 66-416 ms. Velichkovsky et al. (2000; 2005) teilen darüber hinaus in lange und kurze Fixationen ein. Die Grenze dafür liegt bei 180 ms (innerhalb einer Region von ca. 5° des Sehwinkels). In der DIN EN ISO 15007-1: 2015-03 zur Messung des Blickverhaltens von Fahrern bei Fahrzeugen mit Fahrerinformations und -assistenz-systemen ist eine Dauer individueller Fixationen von 100-2000 ms angegeben. Zusätzlich ist vermerkt, dass eine Dauer von weniger als 100 ms nicht möglich ist.

Die mögliche Zeitspanne einer Fixation scheint damit sehr groß. Eine genaue Definition wird dadurch erschwert, dass Fixationsdauern abhängig davon sind, was gesehen wird. So verschiebt sich beispielsweise die oben genannte Grenze zwischen langen und kurzen Fixationen bei dynamischen Stimuli auf 300 ms (Velichkovsky et al., 2000; Velichkovsky et al., 2005). In Abhängigkeit von der jeweiligen Aufgabe sind unterschiedliche Fixationsdauern bei Rayner (1998) angegeben, wie zum Beispiel 200-250 ms beim Lesen von englischen Texten. Die ungefähre mittlere Fixationsdauer beträgt nach seinen Erkenntnissen: für stilles Lesen 225 ms, beim lauten Lesen 275 ms, bei der visuellen Suche 275 ms, beim Lesen von Musik 375 ms und beim Schreibmaschinenschreiben 400 ms. Laut Ollermann (2004) werden beim figurativen Verarbeiten von Bildern Fixationsdauern von 120-250 ms erreicht. In seiner Studie, bei der die Aufgabe zu einer schnellen visuellen Abtastbewegung führte, lag die mittlere Fixationsdauer bei 186 ms und mehr als zwei Drittel der Fixationen dauerten weniger als 200 ms. Von Seiten des Eye Tracking Kompetenzzentrums in Zürich erfährt man, dass eine Fixation 100-600 ms dauert, beim Lesen 100-300 ms, beim Suchen und Orientieren 100-200 ms und beim Studieren von Details 300-600 ms erreicht werden (Zimmermann, 2014). Alle hier aufgeführten Erkenntnisse sind in Tabelle 2 zusammengefasst. Abhängig davon, welche Grenzen zur Identifizierung von Fixationen

vorgegeben werden, können Interpretationen bezüglich kognitiver Verarbeitung stark variieren (Poole & Ball, 2006).

Tabelle 2. Angaben in der Literatur bezüglich der Beschreibung von Fixationen.

Autor(en)	**Geschwindigkeit**	**Dauer**	**Streuung**
Salvucci und Goldberg (2000)	<100°/s	110-200 ms	0,5-1°
Holmqvist et al. (2011)	10-50°/s	mind. 50-250 ms	0,5-2,0°
Granka et al. (2004)		ca. 200-300 ms	bestimmtes Areal des visuellen Feldes
Jacob & Karn (2003)	<15-100°/s	100-200 ms	~2°
Sibert & Jacob (2000)		mind. 100 ms (200-600 ms)	0,5°
Taylor et al. (2015)	15-100°/s	100-200 ms	2°
Pan et al. (2004)		mind. 200 ms	40px Radius
Ollerman (2004)		mind. 100 ms Verarbeitung Bilder: 120-250 ms	12pt
Rayner (1998)		200-300 ms Englisch lesen: 200-250 ms	
Goldberg (2002)		200-400 ms	
Loftus & Mackworth (1978)		ca. 300 ms	
Wade & Tatler (2005)		ca. 300 ms	
Poole & Ball (2006)		66-416 ms; Durchschnitt 218 ms	
Velichkovsky et al. (2000; 2005)		statisch: kurze Fixation < 180 ms > lange Fixation dynamisch: kurze Fixation < 300 ms > lange Fixation	5°
DIN EN ISO 15007-1		(mind.) 100-2000 ms	
Zimmermann (2014)		100-600 ms Lesen: 100-300 ms Suchen & Orientieren: 100-200 ms Studieren v. Details: 300-600 ms	

Die andere wichtige Messgröße bezüglich der Blickbewegungen stellen die sogenannten Sakkaden dar. Bei Sakkaden handelt es sich um kurze, schnelle Augenbewegungen, die zwischen den Fixationen stattfinden (z. B. Goldberg et al., 2002; Rayner, 1998). Sie stellen die schnellste Bewegung dar, zu welcher der menschliche Körper im Stande ist und werden anhand von Geschwindigkeit oder

Beschleunigungsschwellen definiert (Holmqvist et al., 2011). Dabei können Geschwindigkeiten von über 500°/s erreicht werden (Pan et al., 2004). Die gängigen Grenzen zur Erkennung von Sakkaden liegen dabei bei einer Geschwindigkeit von 30-100°/s und einer Beschleunigung von 4000-8000°/s² (Holmqvist et al., 2011). Salvucci & Goldberg (2000) verwenden beispielsweise eine Schwelle von >300°/sek, ab der sie in ihren Daten von einer Sakkade ausgehen. Der während einer Sakkade zurückgelegte Weg reicht laut DIN EN ISO 15007-1 von 1° beim Lesen eines Textes bis zu 5° während der Betrachtung einer Szene. Laut Sibert & Jacob (2000) wird sogar eine Fläche von 1-40° des Sehwinkels (durchschnittlich 15-20°) abgedeckt. Als Dauer der Sakkaden geben sie 30-120 ms an. Andere Angaben machen hier Poole & Ball (2006) mit 20-35 ms, Holmqvist et al. (2011) mit 30-80 ms und Taylor et al. (2015) mit 20-100 ms. Entsprechend den Fixationen ist die Dauer dabei abhängig vom experimentellen Kontext (Taylor et al., 2015) bzw. der Distanz, die während einer Sakkade überbrückt wird (Rayner, 1978, 1978). So dauert eine Sakkade über 2°, wie sie typischerweise beim Lesen entsteht, ca. 30 ms, während eine 5° Sakkade, bei der Wahrnehmung einer Szene ungefähr 40-50 ms dauert (Rayner, 1998). Laut Velichkovsky (2000; 2005) besteht zudem eine systematische Kombination zwischen der Amplitude der Sakkade und der vorangegangenen Fixation. Nach Fixationen von 90-260 ms folgten in deren Versuchen Sakkaden von mehr als 5°, während Fixationen länger als 260-280 ms hauptsächlich Sakkaden einleiteten, die unter 5° lagen. Diese unterschiedlichen Muster in den Blickbewegungen werden unterschiedlichen Aufmerksamkeitsmodi zugeordnet (Velichkovsky et al., 2000). So werden zu Beginn der Betrachtung einer Szene Objekte mit kurzen Fixationen und langen Sakkaden lokalisiert. Dieser Modus wird *Umgebungsmodus* (*ambient mode*) genannt (Helo et al., 2014). Die Identifizierung von Objektdetails, die sich in längeren Fixationen und kürzeren Sakkaden niederschlägt, wird dagegen als *fokaler Modus* (*focal mode*) bezeichnet. Eine Kombination aus Fixationen und Sakkaden wird bei der sogenannten Verweilzeit (*dwell time*) verwendet. In der Forschung wird diese Größe auch als Blick (*gaze* (Rayner, 1998) oder *glance* (Green, 2002) bezeichnet (Jacob & Karn, 2003). Welche Blickereignisse genau in diese zusammenfassende Größe einbezogen werden, unterscheidet sich häufig (Green, 2002). Allen Variationen gemeinsam ist aber die Eingrenzung auf ein bestimmtes Interessengebieten innerhalb des visuellen Feldes (DIN EN ISO 15007-1; Salvucci & Goldberg, 2000), der sogenannten *area of interest* (AOI). Dabei stellen AOIs beliebig definierte Flächen dar, die Objekte beinhalten, die für die jeweilige Studie von Interesse sind (Goldberg et al., 2002). Laut DIN EN ISO 15007-1 darf dieses die normale Auflösung des verwendeten Blickerfassungssystems nicht unterschreiten. In derselben Norm wird außerdem zwischen der Verweilzeit (*dwell time*) und dem Blick (*glance*) unterschieden. Als Verweilzeit wird dabei die Summe aller aufeinanderfolgenden Fixationen und Sakkaden bis zu dem Zeitpunkt, an dem die Augenbewegung vom Interessengebiet wegführt, definiert. Bei der Berechnung der Blickdauer wird dem noch die Zeit hinzugefügt, in der der Blick sich dem jeweiligen AOI zugewendet hat. Für die Konstrukte *gaze* von Poole und Ball (2006) und Taylor (2015), bzw. *gaze duration* von Rayner (1998) und Duchowski (2002) wurden dagegen nur die Fixationen innerhalb der Interessengebiete summiert. Dem schließt sich auch die Beschreibung der *gaze duration* von Jacob & Karn (2003) an, die allerdings erwähnen, dass auch die kurzen Sakkaden zwischen diesen Fixationen einbezogen werden können. Etwas ungenauer ist die Verweilzeit bei Holmqvist et al. (2011) als das Verweilen des Blickes innerhalb einer AOI von Eintritt zu Austritt definiert. Sie geben darüber hinaus an, dass die Verweilzeit ihre eigenen Maße wie Dauer, Startzeitpunkt, Streuung usw., ähnlich einer Fixation besitzt, mit dem Unterschied, dass die Verweilzeit bezogen auf Zeit und Raum größer ist. Prinzipiell wird dieses wissenschaftliche Konstrukt der Verweilzeit u. a. genutzt, um Aussagen über die Aufmerksamkeitsverteilung zwischen unterschiedlichen Interessensgebieten machen zu können (Poole & Ball, 2006). Laut DIN EN ISO 15007-1 liegen typische Blickdauern im Bereich von 500 ms bis zu 3 s und variieren in Abhängigkeit von Stimulus und Aufgabe.

2.5.4 Blickbewertung

Blickbewegungen entstehen nicht zufällig (Heidmann & Ziegler, 2002). Während der Sakkaden wird der Blick auf die Areale gelenkt, die den höchsten Informationsgehalt haben (Heidmann & Ziegler, 2002). Dort kann dann Informationsaufnahme und –verarbeitung stattfinden (Granka et al., 2004). Wenn ein Objekt wichtig erscheint, wird es für gewöhnlich fixiert (Duchowski, 2002). Mittels der Aufnahme von Blickbewegungen kann somit dynamisch nachvollzogen werden, wo, bezogen auf einen visuellen Stimulus, die Aufmerksamkeit einer Person lag (Poole & Ball, 2006).
Heidmann und Ziegler (2002) stellen einige Variablen der Blickbewegungsregistrierung vor, die auf Basis von Fixationen berechenbar sind. So könnte man sich zunächst einmal ansehen, wo Fixationen verortet sind. Ist ein bestimmtes Objekt von Interesse, stellt sich die Frage, ob dieses wahrgenommen wurde oder nicht. Falls Fixationen in den Bereich dieses Objektes fallen, kann die Fixationsdauer analysiert werden. Auch die Häufigkeit von Fixation auf einem oder mehreren Objekten kann von Interesse sein, sowie die Reihenfolge, in der diese stattfanden. Abhängig vom Inhalt der Studie ist es möglich, dass auch Maße der Sakkaden wie Sakkadenlänge oder Sakkadenhäufigkeit aufschlussreiche Variablen darstellen. Darüber hinaus können auch Negativaussagen, darüber, was nicht angeschaut wurde, gemacht und analysiert werden (Oehme & Jürgensohn, 2006). Die Anzahl der in der Literatur verwendeten Messgrößen ist sehr groß, was daran liegt, dass eine standardisierte Terminologie und Definitionen für die fundamentalen Konzepte fehlen (Jacob & Karn, 2003). Wichtig ist, welche Schlüsse aus diesen Variablen gezogen werden. Die Interpretation hängt dabei stark vom jeweiligen Kontext ab (Poole & Ball, 2006). So kann anhand einer hohen Fixationshäufigkeit entweder auf höheres Interesse am Zielobjekt geschlossen werden oder die Häufigkeit der Fixationen durch die Komplexität des Objektes bedingt sein (Poole & Ball, 2006). Gleichsam kann dieses aber auch sehr komplex oder aufwändig zu entschlüsseln sein. Prinzipiell kann bei der Datenanalyse nach dem *top-down* oder dem *bottom-up* Prinzip vorgegangen werden (Jacob & Karn, 2003). Beim Vorgehen nach dem *top-down* Prinzip werden die Daten basierend auf einer kognitiven Theorie oder Hypothese analysiert um Aspekte des Modells stützen oder verwerfen zu können (Goldberg et al., 2002). Rückschlüsse auf Basis beobachteten Verhaltens werden beim *bottom-up* Prinzip gezogen (Goldberg et al., 2002). Laut Jacob & Karn (2003) stellen die Gesamtzahl aller Fixationen, der Anteil der Blickdauern pro AOI, der Mittelwert der gesamten Fixationen, die Anzahl der Fixationen pro AOI, die mittlere Blickdauer pro AOI und die Fixationsrate (Fixationen/s) die Messgrößen dar, die am häufigsten verwendet werden. Bezüglich des Anteils der Blickdauern pro AOI weisen sie darauf hin, dass die darin verrechneten Größen Häufigkeit und Dauer der Blickzuwendungen lieber separat verwendet werden sollten. Bezugnehmend auf Fitts, Jones und Milton (1950) kann aus der Dauer dann auf die Schwierigkeit der Informationsextraktion und aus der Häufigkeit auf die relative Wichtigkeit dieser AOI geschlossen werden. Dabei halten Jacob & Karn (2003) die *gazes*, in diesem Fall die Summe aufeinanderfolgender Fixationen innerhalb einer AOI für aussagekräftiger als einzelne Fixationen. Ihrer Meinung nach stellen die Schwierigkeiten die Blickbewegungsdaten mit kognitiver Aktivität zu verknüpfen, die größte Hürde dar, Blickbewegungs-analysen in Studien zu implementieren. Auch Oehme & Jürgensohn (2006) erwähnen das Risiko der Überinterpretation von Ergebnissen.

2.5.5 Vor- und Nachteile des Verfahrens

Die 2003 von Jacob und Karn noch beschriebene Schwierigkeit der aufwändigen Extraktion von Ereignissen aus der Vielzahl der Daten der Blickbewegung ist dagegen heute weniger ein Problem.

Heidmann und Ziegler kamen (2002) noch zu dem Schluss, dass die „aus Eye Tracking Daten gewonnenen Erkenntnisse […] in keinem Verhältnis zum notwendigen Aufwand“ stehen (S. 54). Die heutigen Systeme übernehmen sehr viel mehr dieser Arbeiten. Auch ein anderes von Jacob & Karn (2003) genanntes Problem, nämlich die Einschränkung, dass es einer physikalischen Verbindung zwischen Proband und Eye-Tracker bedarf, wurde in den letzten Jahren zumindest teilweise gelöst (Heidmann & Ziegler, 2002). So ist es heute dank sogenannter Remote Systeme möglich, Blickbewegungen berührungslos zu erfassen (Holmqvist et al., 2011). Auch für die Schwierigkeiten, die sich daraus ergeben, dass der normale Weg der benötigten Reflektionen unterbrochen wird (Poole & Ball, 2006), gibt es heute Lösungen. So konnten häufig die Blickbewegungen von Probanden, die viel Mascara, eine Brille oder Kontaktlinsen trugen, hängende Augenlider oder zu feuchte Augen hatten, nicht erfasst werden (Holmqvist et al., 2011). Dieses Problem umgehen neue Eye-Tracker, indem die Augen ohne Infrarotreflektionen mit einer Videokamera aufgezeichnet werden und das System Pupille und Linse mittels Bilderkennungssoftware erkennt (z. B. Dikablis Glasses der Ergoneers GmbH). Die stärkste Hemmschwelle bezüglich der Verwendung von Blickbewegungsanalyse-Verfahren sehen Heidmann und Ziegler (2002) in den hohen Anschaffungskosten der Systeme. Holmqvist et al. (2011) zeigen auf, dass heutige Nutzer darüber hinaus vor der Schwierigkeit stehen, sich aus vielen verschiedenen Geräten von vielen Anbietern das herauszusuchen, mit dem sich ihre Vorstellungen auch wirklich umsetzen lassen. Ein Vorteil der Erfassung von Blickbewegungsparametern bleibt die Tatsache, dass sie „stark gewohnheitsorientiert und wenig willentlich beeinflusst (z. B. Leven 1986)“ sind (Oehme & Jürgensohn, 2006, S. 3).

Fazit

Bereits seit Ende des 19. Jahrhunderts wird die Methode der Blickbewegungsanalyse eingesetzt. Mit Hilfe von Brillen oder freistehender Systeme werden dabei Augenmerkmale und –bewegungen aufgezeichnet, die dann bezüglich Größen wie beispielsweise Fixationen und Sakkaden untersucht und auf bestimmte Felder im visuellen Feld bezogen werden. Man verspricht sich davon, möglichst gewohnheitsbedingte und willentlich wenig beeinflussbare Messgrößen zu erfassen, welche direkte Rückschlüsse auf sonst schwer erfassbare Variablen wie, Informationsaufnahme, kognitive Verarbeitungstiefe, Interesse oder Grad an Erregung, zulassen.

2.6 Zusammenfassung und Forschungsfragen

Ein Großteil der deutschen Bevölkerung nutzt das Internet (Initiative D21, 2018) und sieht sich dort mit unterschiedlichen Risiken konfrontiert (siehe Kapitel 2.2). Der Fokus dieser Arbeit liegt dabei auf Risiken, welche die personenbezogenen Daten der Nutzer im Kontext des Onlineshoppings betreffen (siehe Kapitel 2.2.1-2.2.3). Zwar bieten verschiedene Gesetze und auch technische Maßnahmen Möglichkeiten, diese personenbezogenen Daten zu schützen (siehe Kapitel 2.3.1 und 2.3.2), jedoch stellt das (sichere) Verhalten der Nutzer den effektivsten Schutz dar (siehe Kapitel 2.3.3).
Menschliches Verhalten und insbesondere Verhalten in Risikosituationen ist Grundlage unterschiedlichster Theorien und Modelle (siehe Kapitel 2.4.1). Dies ergibt sich auch aus der Tatsache, dass Risikoverhalten sehr kontextspezifisch ist (Byrnes et al., 1999). Um Aussagen bezüglich eines bestimmten Verhaltens in einer bestimmten Situation machen zu können, muss dieses demnach in einer entsprechenden Situation erhoben worden sein (Fishbein & Ajzen, 2011). Hinzu kommt, dass die Untersuchung von Risikoverhalten der Einschränkung unterliegt, dass Teilnehmer an Studien keiner

wirklichen Gefahr ausgesetzt sein dürfen (Döring & Bortz, 2016). Dies gewährleistet z. B. eine Erfassung mittels Fragebogen. Zu beachten ist dabei aber, dass in diesem Fall bestenfalls die vorangehende Intention ein Verhalten zu zeigen, manchmal auch angegeben als „Wahrscheinlichkeit das Verhalten zu zeigen“, erfasst werden kann. Im Kontext des Datenschutzes, bzw. der Datensicherheit konnte allerdings schon mehrfach nachgewiesen werden, dass das, was die Menschen tun, nicht dem entspricht, was sie sagen (siehe Kapitel 2.4.2). Unterschiedliche Studien untersuchten zwar sogenanntes Datenschutz-Verhalten im Sinne von Anzahl und Umfang preisgegebener Daten (siehe Kapitel 2.4.3), jedoch bezog sich keine der gefundenen Studien speziell auf Verhalten, welches zum Schutz der persönlichen Daten im Kontext des Online-Shoppings gezeigt wird. Zusätzlich unterliegen die meisten der gefundenen Studien Limitationen, die gefundene Erkenntnisse zumindest einschränken. Dazu gehört z. B., dass nur Fake-Accounts und nicht die tatsächlichen personenbezogenen Daten verwendet wurden, dass die Situation durch vorgegebene Produkte oder Webshops wenig realistisch war oder die Stichprobe gewissen Einschränkungen unterlag. Aus der dargestellten Relevanz des Themas, des eingeschränkten Forschungsstandes in diesem speziellen Kontext und der Zielsetzung dieser Arbeit, ergibt sich

Forschungsfrage 1: Wie lässt sich tatsächliches Datenschutz-Verhalten beim Onlineshopping empirisch erfassen?

Zur Beantwortung dieser Frage ist es notwendig, sich mit folgenden untergeordneten Fragen auseinanderzusetzen:

Forschungsfrage 1a: Wie kann tatsächliches Datenschutz-Verhalten beim Onlineshopping operationalisiert werden?
Forschungsfrage 1b: Wie kann erhobenes Verhalten für weitere Analysen quantifiziert werden? und
Forschungsfrage 1c: Welche Anforderungen bestehen an eine solche empirische Erhebung?

Die empirische Erfassung des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping ermöglicht dann die Analyse dessen als abhängige Variable. Einflussfaktoren auf das tatsächliche Datenschutz-Verhalten können somit ermittelt werden. Als potentielle Einflussfaktoren können die in Kapitel 2.4.1 im Rahmen von Theorien und Modellen vorgestellten unabhängigen Variablen angesehen werden. Der Fokus im Rahmen dieser Arbeit liegt dabei auf Faktoren, die sich ausschließlich in der Person der Nutzer begründen. Bezugnehmend auf die vorgestellte Unabhängigkeit zwischen Intention und dem Verhalten (vergleiche Privacy Paradoxon Kapitel 2.4.2), ergibt sich hieraus

Forschungsfrage 2: Welche personenbezogenen Faktoren haben einen Einfluss auf das tatsächliche Datenschutz-Verhalten beim Onlineshopping?

Mit Hilfe der eventuell gefundenen personenbezogenen Faktoren, die einen Einfluss auf das tatsächliche Datenschutzverhalten ausüben, sollte es möglich sein, ein entsprechendes Modell zur Vorhersage dessen aufzustellen, was im Rahmen der unter Forschungsfrage 1 erarbeiteten Methodik analysiert werden kann. Dabei interessiert insbesondere

Forschungsfrage 3: Inwieweit lässt sich das tatsächliche Datenschutz-Verhalten beim Onlineshopping mit Hilfe der gefundenen Einflussfaktoren vorhersagen?

Wie bereits in der Zielsetzung dieser Arbeit erwähnt, könnte das Wissen um Einflussgrößen auf das Datenschutz-Verhalten beim Onlineshopping zur Ableitung eventueller Gestaltungskriterien möglicher Unterstützungen für Nutzer in diesem Kontext verwendet werden.

Die Beantwortung der aufgestellten Forschungsfragen findet in den nun folgenden Kapiteln statt. Dabei widmet sich Kapitel 3 den Grundlagen zur empirischen Erfassung von Datenschutz-Verhalten beim Onlineshopping (Forschungsfrage 1). In Kapitel 4 werden potentielle Einflussfaktoren auf ebendieses Verhalten untersucht (Forschungsfrage 2) und Kapitel 5 beschäftigt sich mit der Möglichkeit der Vorhersage dieses Verhaltens mittels der gefundenen Einflussfaktoren (Forschungsfrage 3).

3 Vorgehen zur empirischen Erfassung von Datenschutz-Verhalten beim Onlineshopping

Entsprechend der in Kapitel 2.6 erarbeiteten Forschungsfrage 1 *(Wie lässt sich tatsächliches Datenschutz-Verhalten beim Onlineshopping empirisch erfassen?),* soll im Rahmen dieses Kapitels eine Methode entwickelt werden, mit der tatsächliches Datenschutz-Verhalten beim Onlineshopping empirisch erfasst werden kann. Dazu setzt sich Kapitel 3.1 mit der möglichen Operationalisierung dieser Variable auseinander, bevor in Kapitel 3.2 eine durchgeführte Gewichtungsstudie zur Quantifizierung dessen beschrieben wird. Im Anschluss werden, aufbauend auf in Kapitel 2.4.3 gefundenen Einschränkungen, denen bisherige Studien unterliegen, in Kapitel 3.3 Anforderungen an eine empirische Erhebung des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping abgeleitet.

3.1 Operationalisierung von tatsächlichem Datenschutz-Verhalten

Wie in Kapitel 2.1.4 dargelegt, ist Datenschutz-Verhalten beim Onlineshopping im Rahmen dieser Arbeit definiert als eine Sammlung von Handlungen, die Nutzer im Kontext von Onlineshopping zeigen, die das Ziel haben, die eigene Person und deren Privatsphäre zu schützen, indem die eigenen personenbezogenen Daten geschützt werden.
Um im Rahmen einer Studie mit einer Variable *tatsächliches Datenschutz-Verhalten beim Onlineshopping* rechnen zu können, muss zunächst repräsentatives Verhalten, bzw. eine Sammlung von Handlungen (siehe Kapitel 2.1.2) gefunden werden, die dann als Indikatoren im Rahmen eines Messinstrumentes gelten (Döring & Bortz, 2016). Im nächsten Schritt müssen diese Handlungen, bzw. das gezeigte Verhalten in entsprechende Werte übersetzt werden. Diese Werte müssen jenes Verhalten angemessen repräsentieren. Es gilt in diesem Fall demnach ein Maß zu finden, welches angibt, inwieweit jemand seine persönlichen Daten und damit die eigene Person im Rahmen von Onlineshopping schützt.
Möglichkeiten, den Schutz der personenbezogenen Daten beim Onlineshopping zu gewährleisten, wurden in Kapitel 2.3 dargestellt. Die Absicherung durch den Staat stellt dabei keine aktive Handlung des Nutzers dar und muss deshalb im Zuge der Operationalisierung ausgeschlossen werden. Der Schutz der Daten mit Hilfe technischer Möglichkeiten würde sich dagegen in überprüfbare Handlungen wie die Verwendung einer Firewall, eines Browser Add-Ons oder der Überprüfung einer Webseite auf Sicherheitslücken übersetzen lassen. Allerdings wäre hier der Nachteil, dass zur Überprüfung dessen entweder der private Rechner eventueller Probanden in Augenschein genommen werden oder diese Erkenntnisse abgefragt werden müssten. Ersteres soll aus ethischen Gründen vermieden werden und zweiteres würde nicht der Erfassung tatsächlichen Verhaltens (im Gegensatz zu Befragung) entsprechen. Als vielversprechender erweisen sich die in Kapitel 2.3.3 angerissenen Inhalte zu sicherem Verhalten im Kontext des Onlineshoppings. Im Rahmen eines Versuches kann die Anwendung dieser durch die Nutzer überprüft werden. Die Anzahl der vor Angabe der Daten geprüften Hinweise und die Dauer der Überprüfung sollen deshalb im Rahmen der vorliegenden Arbeit als Maß für das jeweilige Datenschutz-Verhalten dienen. Das folgende Kapitel gibt einen Überblick über hierfür verwendbare Hinweise.

3.1.1 Hinweise zur Einschätzung der Vertrauenswürdigkeit eines Webshops

Wie in Kapitel 2.3.3 beschrieben, gibt es Hinweise auf der Webseite eines Webshops, die dem potentiellen Nutzer einen ersten Eindruck über den Umgang des Anbieters mit personenbezogenen Daten und der Sicherheit der Datenübertragung ermöglichen. Im Rahmen dieses Kapitels werden solche Hinweise mit Hilfe unterschiedlicher Quellen zusammengefasst. Der Internetauftritt des Bundesamts für Sicherheit in der Informationstechnik (BSI) weist die Bürger darauf hin, vor Eingabe ihrer Daten zu überprüfen, ob der jeweilige Händler eine vollständige Anbieterkennzeichnung bietet (Bundesamt für Sicherheit in der Informationstechnik, o.D.b). Dazu gehört, dass neben dem Namen, dem Vornamen und der vollständigen Anschrift des Anbieters auch Informationen zur schnellen Kontaktaufnahme, das Gewerberegister, bzw. die Gewerberegisternummer, der Unternehmensname inklusive der Rechtsform und die Umsatzsteuer-Identifikationsnummer auf den Seiten des Webshops zu finden sind. Darüber hinaus sollten die Allgemeinen Geschäftsbedingungen, Informationen zum Umgang mit Datenschutz und Datensicherheit und Informationen zu Widerrufsrecht, Rückgaberecht und Kaufpreis-rückerstattungen vorhanden sein. Weitere wichtige Kriterien sind, welche Zahlungsmöglichkeiten es gibt, ob sämtliche Zusatzkosten transparent dargestellt sind, ob die Angabe https, bzw. ein EV-SSL-Zertifikat vorhanden ist, oder, ob der Webshop Gütesiegel vorweisen kann. Auch die Beurteilung des Webshops durch andere Kunden wird als wichtiger Hinweis genannt.
Neben der Webseite des BSI wurde die Prüfliste der Trusted Shops GmbH als vielversprechende Quelle für aussagekräftige Hinweise gesehen, die der Autorin auf Anfrage ausgehändigt wurde. Jedoch enthält diese überwiegend Prüfkriterien, die von Experten mit dahinterstehenden und internen Bewertungs-kriterien abgeprüft werden und somit in diesem Rahmen wenig zusätzlich Informationen bringen. Auf der Webseite der Trusted Shops GmbH (Trusted Shops GmbH, 2016) sind einige Hinweise dargestellt, die Nutzern helfen sollen unseriöse Online-Händler zu erkennen. Sie entsprechen im Allgemeinen den vom BSI genannten Hinweisen. Ergänzt wurde die im Rahmen dieser Arbeit erarbeitete Liste durch die Doktorarbeit „Erfolgsfaktoren einer E-Commerce-Webseite“ von Dennis Arholdt (2010). In dieser identifiziert er Indikatoren auf Seiten von Webshops, die sich positiv auf die Vertrauensbildung bei Kunden auswirken und quantifiziert deren Auswirkungen. Hinweise von Boos (2015), Downs et al. (2006), Ye, Smith und Anthony (2005) und Kumaraguru, Acquisti und Cranor (2006) wurden außerdem ergänzt.
Insgesamt ergab sich aus diesen Quellen eine Liste mit 40 potentiellen Hinweisen auf die Vertrauenswürdigkeit, bzw. den Umgang mit personenbezogenen Daten. Nicht miteinbezogen wurden die Hinweise, die erst nach Dateneingabe erkennbar/relevant sind (z. B. die Überprüfung, ob die Kreditkartennummer unkenntlich gemacht wurde), die, die eigentlich auf anderen Webseiten liegen (z. B. Recherchieren über Suchmaschinen) und solche, die einer Beurteilung bedürfen (z. B. Rechtschreibefehler, unsinniger Fülltext, Kontakt auf schlechtem Deutsch/Englisch und ungewöhnlich aussehender Bankverbindung). Die sich ergebende Liste ist im Tabelle 3 zusammen mit der Angabe der jeweiligen Quelle und eventueller kurzer Erläuterung dargestellt.

Tabelle 3. Hinweise zur Einschätzung der Vertrauenswürdigkeit eines Webshops.
(Quellen: Polizei Niedersachsen, o.D. = 1; Bundesamt für Sicherheit in der Informationstechnik, o.D.b = 2; Boos, 2015 = 3; Ahrholdt, 2010 = 4; Downs et al., 2006 =5; Ye et al., 2005 =6; Kumaraguru et al., 2006 =7)

Hinweis	**Inhalt (Quelle)**
Allgemeine Geschäftsbedingungen	fehlende oder fehlerhafte AGB können auf Fakeshop hinweisen (1,2,3)
Angaben zu Rücksendekosten	Vorhandensein ist ein Hinweis auf Vertrauenswürdigkeit (2)
Angaben zu Versandkosten	Klare Darstellung ist ein Hinweis auf Vertrauenswürdigkeit (1,2)
Angaben zu Widerrufsrecht	Vorhandensein ist ein Hinweis auf Vertrauenswürdigkeit (2)
	Dem Verbraucher ist „bei einem Fernabsatzvertrag gemäß § 312g Abs. 1 Alt. 2 BGB grundsätzlich auch ein Widerrufsrecht nach § 355 BGB einzuräumen“ (3, S. 69)
Auftragsstatusanzeige/ Sendungsverfolgung	Möglichkeit der Sendungsverfolgung ist ein Hinweis auf Vertrauenswürdigkeit (1)
Bestellfortschrittsanzeige	Potenziell vertrauensförderndes Signal (4)
Besucherzähler	"kann als Qualitätsindikator des Anbieters betrachtet werden" (4, S.76)
Bonusprogramm (z. B. Payback)	Potenziell vertrauensförderndes Signal (4)
EV-SSL-Zertifikat	Hinweis auf SSL-Zertifikat von unabhängigen Zertifizierungsstellen (Verschlüsselte Verbindung), sollte aber überprüft werden (2,5,7)
Expertenbeurteilungen, Testberichte, Preise…	Potenziell vertrauensförderndes Signal (4)
FAQ bzw. Hilfesektion	Potenziell vertrauensförderndes Signal (4)
Firmeninformationen (Wir über uns)	Potenziell vertrauensförderndes Signal (4)
Garantien	Potenziell vertrauensförderndes Signal (4)
Gewerberegister und –nummer	Vorhandensein ist ein Hinweis auf Vertrauenswürdigkeit (2)
Großes Artikelsortiment	Potenziell vertrauensförderndes Signal (4)
Gütesiegel	Gütesiegel sind ein Hinweis auf Vertrauenswürdigkeit, sollten allerdings überprüft werden (1,2,3,4)
Hinweis auf Rückgaberechte	Vorhandensein ist ein Hinweis auf Vertrauenswürdigkeit (2)
Hinweis MwSt., bzw. USt.	Klare Darstellung ist ein Hinweis auf Vertrauenswürdigkeit (2)
https in URL	weist auf verschlüsselte Verbindung hin (2,6,7)
Individuelle Accounts/ Benutzer Log-Ins	Potenziell vertrauensförderndes Signal (4)
Informationen zum Datenschutz, -sicherheit	Vorhandensein ist ein Hinweis auf Vertrauenswürdigkeit (2)
Informationen zur schnellen Kontaktaufnahme	Vorhandensein ist ein Hinweis auf Vertrauenswürdigkeit (2)
	Art. 246a § 1 Abs. 1 Nr. 2 EGBGB fordert die Angabe der Identität des Anbieters, wie Kontaktmöglichkeiten (3)
Internetbezahlsysteme (z. B. Paypal)	Potenziell vertrauensförderndes Signal (4)

Hinweis	**Inhalt (Quelle)**
Klare Preisangabe	ungewöhnlich günstiger Preis kann auf Fakeshop hinweisen (1)
	Transparenz von Zusatzkosten ist ein Hinweis auf Vertrauenswürdigkeit (2)
	„Nach Nr. 4 HS 1 Alt. 1 muss der Unternehmer auch den Gesamtpreis einschließlich aller Steuern und Abgaben angeben." (3, S.64)
Kundenbeurteilungen des Shops	
Links zu verwandten Websites	Potenziell vertrauensförderndes Signal (4)
Look-in-Feature	Potenziell vertrauensförderndes Signal (4)
Name und Anschrift des Anbieters	Vorhandensein ist ein Hinweis auf Vertrauenswürdigkeit (2)
	Art. 246a § 1 Abs. 1 Nr. 2 EGBGB fordert die Angabe der Identität des Anbieters, also des vollständigen Namens und der Anschrift (3)
Produktbeschreibung	„Nach Art. 246a § 1 Abs. 1 Nr. 1 EBGB sind zunächst die wesentlichen Eigenschaften des Produktes anzugeben" (3, S.63)
Produktbild	Potenziell vertrauensförderndes Signal (4)
Produktempfehlungen	
RSS-Feed	Potenziell vertrauensförderndes Signal (4)
Shopname (URL)	Inkonsistenz Shopname zu Name in URL kann auf Phishing oder Fakeshop hinweisen (1)
	Austausch von O durch 0 oder w durch vv kann auf betrügerische Seite hinweisen (5)
Social Bookmarks	Potenziell vertrauensförderndes Signal (4)
Sprachoptionen	„Nach Art. 246c Nr. 4 EGBGB muss der Kunde auch über alle Sprachen informiert werden, in denen der Vertrag abgeschlossen werden kann." (3, S.78)
Umsatzsteuer-Identifikationsnummer	Vorhandensein ist ein Hinweis auf Vertrauenswürdigkeit (2)
Unternehmensname und Rechtsformzusatz	Vorhandensein ist ein Hinweis auf Vertrauenswürdigkeit (2)
Verfügbarkeitsanzeige	immer verfügbare Ware kann auf Fakeshop hinweisen (1)
Verschiedene Versandoptionen	Versicherter Versand soll bevorzugt werden (1)
Viele Zahlungsmethoden	Potenziell vertrauensförderndes Signal (4)

Um die potentielle Überprüfung dieser Hinweise im Rahmen einer Studie nachvollziehen zu können, eignet sich das in Kapitel 2.5 vorgestellte Verfahren der Blickbewegungsanalyse. Die Konkretisierung des Messverfahrens bezüglich der hier zu erarbeitenden Erhebungsmethodik ist im Folgenden dargestellt.

3.1.2 Konkretisierung der Blickbewegungsanalyse

Um das Messverfahren der Blickbewegungsanalyse verwenden zu können, ist es notwendig, die zu verwendenden Messgrößen und deren Grenzen genau festzulegen. Da eine Informationsaufnahme im Rahmen der visuellen Wahrnehmung fast ausschließlich während der Fixationen stattfindet (Helo et al., 2014), stellt diese Messgröße die entscheidende, im Rahmen der Überprüfung der oben dargestellten

Hinweise dar. Wie bereits in Kapitel 2.5.3 dargestellt, besteht bezüglich deren Grenzen in der Literatur hierfür nur eingeschränkte Einigkeit. Zur Festlegung einer gestützten eigenen Definition für das zu verwendende Maß der Fixation wurden deshalb die gefundenen und in Tabelle 2 (siehe Kapitel 2.5.3) dargestellten Definitionen für Fixationen visuell auf einem Zeitstrahl abgetragen. Dieser ist in Abbildung 6 dargestellt.

So aufbereitet zeichnet sich eine Untergrenze von 100 ms ab, über die eine gewisse Einigkeit besteht. Eine weitere Grenze zeigt sich bei einer Dauer von 200 ms. Während hier laut einiger Quellen die Dauer einer Fixation endet (Jacob & Karn, 2003; Salvucci & Goldberg, 2000; Taylor et al., 2015), sehen andere hier erst den Beginn intensiverer Beschäftigung. So variieren laut Zimmermann (2014) Fixationsdauern beim Suchen und Orientieren zwischen 100-200 ms, laut Rayner (1998) beginnen sie bei 200 ms, wenn es das Lesen englischer Text betrifft. An der Stelle wird deshalb im Rahmen dieser Studie eine Grenze gezogen, zwischen den Fixationen, die einen kurzen Blick symbolisieren, der das Vorhandensein eines gewissen Interessensgebietes kontrolliert und denen, die für eine eingehendere Beschäftigung damit stehen. Ein kurzer Blick auf ein Interessensgebiet ist demnach eine Fixation, die mindestens 100 ms und höchstens 200 ms dauert. Die eingehendere Betrachtung des Interessensgebietes beginnt dagegen erst dann, wenn der Blick länger als 200 ms verweilt. Die zweite wichtige zu definierende Größe neben der Dauer stellt die erlaubte räumliche Ausdehnung der Blickbewegung dar. Auch diesbezüglich werden in der Literatur unterschiedliche Angaben gemacht (siehe Kapitel 2.5.3). Um die gesammelten Angaben vergleichen zu können, mussten die verwendeten Einheiten angeglichen werden. So geben die meisten Quellen das Maß der Ausdehnung in ° Sehwinkel an, Pan et al. (2004) verwenden dagegen eine Grenze von einem Radius von 40 px und Ollerman (2004) von 12 pt.

Als maximale Ausdehnung wird in dieser Studie das Maß von 2° Sehwinkel oder entsprechend 87 px festgelegt.

Die beiden Werte für die Mindestdauer einer Fixation und die maximale Ausdehnung bilden dann die Grundlage für den im Rahmen der Blickbewegungsanalyse verwendeten Algorithmus.

Um den Blickbewegungsmaßen inhaltliche Wert zuzuordnen, werden die oben dargestellten Hinweise zum sicheren Onlineshopping als sogenannte Areas of Interests (AOI) verwendet (siehe Kapitel 2.5.3). Beim Legen der entsprechenden Felder wird sich an den Anweisungen von Holmqvist et al. (2011) orientiert. Diese besagen, dass jede AOI eine Fläche mit homogener Bedeutung abdecken soll. Darüber hinaus sollte möglichst darauf geachtet werden, dass die AOI nicht zu klein sind, nicht zu nahe zusammenliegen und Überlappungen nur benutzt werden, wenn die Hypothese oder der Stimulus es notwendig macht. Auch das Verteilen einer AOI über verschiedene Gebiete des Stimulus sollte darin begründet sein. Generell sollten die AOI-Flächen nicht beliebig, sondern so präzise wie möglich positioniert werden.

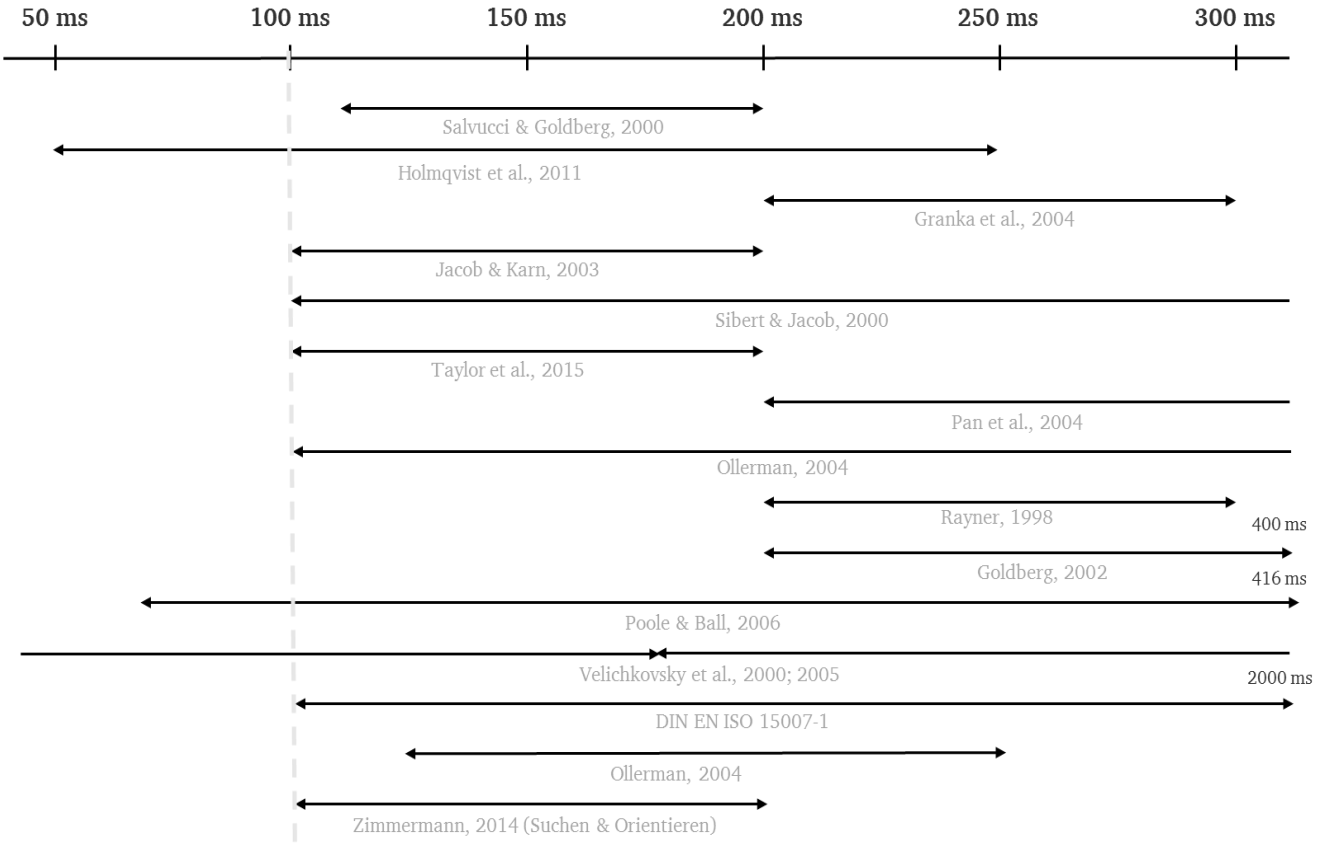


Abbildung 6. Darstellung der in der Literatur gefundenen Definitionen für Fixationen, mit Hilfe eines Zeitstrahls.

3.2 Quantifizierung der aufgezeichneten Daten

Wie in Kapitel 2.3.3 bereits beschrieben, gibt es Hinweise auf der Webseite eines Webshops, die dem potentiellen Nutzer einen ersten Eindruck über den Umgang mit personenbezogenen Daten ermöglichen. Die Anzahl der vor Angabe der Daten geprüften Hinweise und die Dauer dieser Überprüfung sollen im Rahmen dieser Arbeit als Maß für das jeweilige Datenschutz-Verhalten dienen. Es wird davon ausgegangen, dass dabei nicht alle der gesammelten Hinweise gleich wichtig sind, bzw. mit der gleichen Intensität überprüft werden müssen. Antwort darauf, ob das so ist und wenn ja, wie die Gewichtung der einzelnen Hinweise aussieht, soll eine Expertenbefragung im Rahmen einer Gewichtungsstudie bringen. Das Expertenrating gilt bei einer solchen Fragestellung als geeignete Lösung (Döring & Bortz, 2016). Im Folgenden sind Vorgehen (3.2.1), Ergebnisse (3.2.2) und die Diskussion (3.2.3) bezüglich der durchgeführten Studie beschrieben.

3.2.1 Vorgehen Gewichtungsstudie

Die Liste der potentiellen Hinweise auf die jeweilige Vertrauenswürdigkeit auf den Seiten eines Webshops (siehe Kapitel 3.1.1) bildet die Grundlage für diese Untersuchung. Um einen Eindruck über die Vergleichbarkeit der Hinweise im Zuge der Operationalisierung des tatsächlichen Datenschutz-Verhaltens zu bekommen, sollten diese von Experten im Bereich Datenschutz beim Onlineshopping eingeschätzt werden. Dabei wurde vermutet, dass auch die notwendige Intensität der Betrachtung der

Hinweise sich unterscheiden könnte. Während es bei dem Hinweis *https in der Adresszeile* ausreicht, mit einem kurzen Blick das Vorhandensein zu prüfen, sollte es zum Beispiel im Rahmen der *AGB* notwendig sein, mehr Zeit zu investieren, um diese lesen zu können. Die Experten wurden aus diesem Grund gebeten, zum einen einzuschätzen, wie wichtig es ist, mit einem kurzen Blick zu überprüfen, ob der jeweilige Hinweis vorhanden ist oder nicht. Zum anderen sollten sie für den gleichen Hinweis angeben wie wichtig es ist, sich darüber hinaus eingehender mit demselben Hinweis zu beschäftigen.
Diese Einschätzung geschah dann für alle Hinweise mittels einer visuellen Analogskala. Bei der visuellen Analogskala handelt es sich um eine „kontinuierliche Skala ohne konkrete Skalenstufen" (Moosbrugger & Kelava, 2007, S. 51). Diese führt zu intervallskalierten Ratings (Döring & Bortz, 2016). Die Teilnehmer werden dabei gebeten auf einer Linie die entsprechende Stelle zwischen zwei Antwortankern zu markieren, die ihrer Antwort auf das jeweilige Item entspricht. Im Hintergrund waren die Werte 1-100 hinterlegt. Diese konnten von den Experten nicht wahrgenommen werden. Links von jeder Skala waren zwei unterschiedliche Regler zu sehen, welche die Experten an die entsprechende Stelle zwischen „unwichtig" (links der Skala) und „wichtig" (rechts der Skala) schieben sollten, die die jeweilige Wichtigkeit repräsentiert. Der eine Regler stellt ein Auge dar und sollte die Kategorie des kurzen Blickes repräsentieren. Das verwendete Bild ist frei im Internet erhältlich (freepik.com, o.D.). Der zweite Regler stellt eine Leselupe dar. Diese sollte die eingehendere Beschäftigung verbildlichen. Das Symbol dafür wurde selbst erstellt. Beide Regler sind in Abbildung 7 dargestellt.

Abbildung 7. Regler im Rahmen der visuellen Analogskala bezüglich der Einschätzung der Wichtigkeit der Hinweise mittels eines kurzen Blickes (Symbol Auge) bzw. einer eingehenderen Beschäftigung (Symbol Leselupe).

Da vermutet wird, dass es nicht zwingend notwendig ist, alle potentiellen Hinweise zu überprüfen, bevor dem Webshop ein gewisses Vertrauen entgegengebracht werden kann, wurden die Experten im nächsten Schritt gebeten, aus dem maximal fünf wichtigsten Hinweisen eine Rangreihe zu bilden. Alle Hinweise waren dafür in einzelnen Kästchen dargestellt. Diese konnten dann einzeln per Doppelklick oder Drag & Drop nach rechts in fünf abgebildete Kästchen verbracht werden, die von oben nach unten mit den Ziffern 1-5 nummeriert waren.
Der gesamte Fragebogen wurde als Online-Fragebogen mit Hilfe des Software-Pakets SoSci Survey (*SoSciSurvey.de,* o.D.) konzipiert und ist in Anhang A dieser Arbeit zu finden. Im Rahmen von wissenschaftlichen Befragungen ohne kommerziellen Hintergrund ist dieses kostenlos nutzbar. Die Online-Befragung konnte über eine URL aufgerufen werden, die potentiellen Teilnehmern zusammen mit dem notwendigen Passwort per Email zugesandt wurde.
Zu Beginn wurden die Experten zunächst begrüßt und der Dank für die Bereitschaft teilzunehmen bekundet. Es folgte eine kurze Einführung in das Thema. Mit einem Klick auf den Weiter-Button wurde dann die nächste Seite geöffnet, auf der die Experten ihre Zustimmung zur anonymisierten Verwendung ihrer Daten im Rahmen dieser Forschung gaben. Darüber hinaus hatten sie die Möglichkeit, ihre Emailadresse zu hinterlassen, um eine Zusammenfassung der Ergebnisse zu erhalten. Es wurde darauf hingewiesen, dass diese Adresse zu keinem Zeitpunkt mit den von ihnen im Rahmen der Befragung gemachten Angaben in Verbindung gebracht wird. Ab diesem Zeitpunkt war neben dem Weiter-Button auch ein Zurück-Button vorhanden, so dass innerhalb der Befragung vor- und zurückgeblättert werden konnte. Im nächsten Schritt füllten die Experten einen Lückentext mit Angaben zu ihrer Person aus.

Darauf folgte zunächst die Beschreibung des Szenarios eines Nutzers, der auf der Webseite eines ihm bislang unbekannten Webshops ein Produkt kaufen möchte, welches in die Einschätzung der Wichtigkeit der verschiedenen Hinweise einleitete. Danach wurde zum anschließenden Ranking übergeleitet. Im Anschluss wurde den teilnehmenden Experten noch einmal für die Teilnahme gedankt und sie hatten in einem freien Eingabefeld die Möglichkeit, jegliche Art von Rückmeldung zu geben.
Bevor die Experten angeworben wurden, fand ein Pre-Test mit 5 Probanden statt. Dieser führte zu kleinen Änderungen. So wurde zusätzlich darauf hingewiesen, dass einzelne Hinweise, die für völlig unwichtig befunden werden bei der Einschätzung der Wichtigkeit, auch übersprungen werden können. Dies hat den Hintergrund, dass die Liste der Hinweise sehr umfassend ist und eine Einschätzung sowohl für einen kurzen Blick, als auch für die eingehendere Beschäftigung recht zeitintensiv ist. Die Probanden sollten vor allem nicht bereits zu Beginn der Befragung unnötig strapaziert werden, da befürchtet wurde, dass sie sonst abbrechen könnten. Die Befragung fand im Zeitraum von Mai bis Juni 2017 statt.
Als potentielle Teilnehmer der Befragung wurden Experten der TU Darmstadt im Rahmen des Themas Datenschutz beim Onlineshopping angeschrieben. Darüber hinaus wurde auch beim amtierenden Hessischen Datenschutzbeauftragten und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und deren Mitarbeiter angefragt. Auch verschiedene Mitarbeiter der Initiative 21 wurden gebeten an der Befragung teilzunehmen.
Die Angaben der Experten im Rahmen der Gewichtungsstudie führen zu wichtigen Ergebnissen. Diese werden unterteilt nach der Wichtigkeit der Überprüfung auf Vorhandensein, bzw. der eingehenderen Beschäftigung der verschiedenen Hinweise (Kapitel 3.2.2.1), dem Ranking der wichtigsten Hinweise (Kapitel 3.2.2.2) und den Ergebnissen bezüglich der Quantifizierung von Datenschutz-Verhalten (Kapitel 3.2.2.3) dargestellt.

3.2.2 Ergebnisse Gewichtungsstudie

Für die Gewichtungsstudie konnten insgesamt 10 Experten gewonnen werden. Aufgrund eines technischen Problems sind die Daten von nur 9 teilnehmenden Experten auswertbar. Diese 9 Experten beschäftigen sich zwischen 2 und 15 Jahren (Median 4 Jahre) mit dem Thema "Datenschutz beim Onlineshopping". Zwei nähern sich der Thematik dabei von technischer, vier von juristischer, zwei von psychologischer (/sozialwissenschaftlicher) und einer von organisatorischer Seite. Im Rahmen des Lückentextes „Ich arbeite zur Zeit als…“ machten die Experten folgende Angaben:

- PostDoc
- Wissenschaftlicher Mitarbeiter
- Datenschutzaufsichtsbehörde
- Beamter der Datenschutzaufsichtsbehörde
- Juristin
- Referent bei der Datenschutzaufsichtsbehörde
- Wissenschaftlicher Mitarbeiter
- Doktorand
- Security Management Consultant

3.2.2.1 Wichtigkeit der Überprüfung auf Vorhandensein, bzw. der eingehenderen Beschäftigung der verschiedenen Hinweise

Für jeden der 40 Hinweise auf den Umgang mit personenbezogenen Daten sollten von den Experten zwei Werte angegeben werden. Einer dieser Werte entspricht dabei der eingeschätzten Wichtigkeit zu überprüfen, ob der Hinweis auf der Webseite vorhanden ist oder nicht. Der andere Wert gibt an, inwieweit es als wichtig eingeschätzt wurde, dass man sich mit eben diesem Hinweis darüber hinaus beschäftigen sollte. Aus den Angaben der 9 Experten wurden daraufhin für jede der Einschätzungen der Mittelwert errechnet. Die erhaltenen Werte sind in Tabelle 4 dargestellt.
Es fällt auf, dass verhältnismäßig hohe Standardabweichungen vorliegen. Bei der Standardabweichung handelt es sich um ein Maß für die Streuung der Werte um den Mittelwert, genauer gesagt: die „Summe der quadrierten Abweichungen aller Messwerte vom arithmetischen Mittel, dividiert durch die Anzahl aller Messwerte“ (Bortz, 2005, S. 41). Diese Uneinigkeit der Experten bei der Einschätzung der Wichtigkeiten zeigt sich auch im oftmals sehr großen Abstand zwischen dem niedrigsten (Min) und dem höchsten (Max) angegebenen Wert. Die Vermutung liegt dabei nahe, dass sich die Unterschiede in der Bewertung aus den unterschiedlichen Fachdisziplinen der Experten ergeben. Eine Analyse dessen zeigte aber keine augenscheinlichen Zusammenhänge.
Als wichtigster Hinweis bezüglich eines kurzen Blickes zur Überprüfung auf Vorhandensein ergab sich *https in URL* (Mittelwert 68,33). Acht von neun Experten stuften diesen Hinweis als vergleichsweise wichtig ein, während ein Experte dessen Überprüfung als unwichtig befand. Dieser Experte räumte jedoch der eingehenderen Betrachtung desselben Hinweises eine hohe Wichtigkeit ein.
Am wichtigsten bezüglich der eingehenderen Betrachtung wurden insgesamt die *Informationen zu Datenschutz/-sicherheit* (Mittelwert 62,11) eingestuft. In diesem Fall wurde die Skala mit Angaben von 0 bis 100 voll ausgenutzt. Bei genauerer Analyse fällt hierbei auf, dass die juristischen Experten die Wichtigkeit des kurzen Blickes höher bzw. in einem Fall genauso hoch, wie die der eingehenderen Betrachtung einstuften. Alle anderen Experten gaben eine eindeutig höhere Wichtigkeit der eingehenderen Beschäftigung an. Einzig ein Experte befand beides als gänzlich unwichtig.

Tabelle 4. Mittelwerte ($\bar{x}$), Standardabweichung (s), Minimum (Min) und Maximum (Max) der Wichtigkeit der Überprüfung auf Vorhandensein (kurzer Blick) und der Wichtigkeit einer eingehenderen Betrachtung (langer Blick) für die Hinweise auf den Umgang mit personenbezogenen Daten auf einer Skala von „unwichtig“ (0) bis „wichtig“ (100).

Hinweis	**Kurzer Blick**				**Langer Blick**			
	$\bar{x}$	**(s)**	**Min**	**Max**	$\bar{x}$	**(s)**	**Min**	**Max**
Allgemeine Geschäftsbedingungen	42,22	28,64	18	100	44,78	26,53	0	84
Angaben zu Rücksendekosten	36,67	29,62	0	88	31,78	35,61	0	100
Angaben zu Versandkosten	41,89	30,19	0	75	31,22	31,06	0	68
Angaben zu Widerrufsrecht	25,33	24,16	0	71	20,11	25,31	0	67
Auftragsstatusanzeige/Sendungsverfolgung	33,22	29,21	0	79	22,22	26,48	0	63
Bestellfortschrittsanzeige	37,89	28,75	0	76	30,22	29,67	0	78
Besucherzähler	3,67	7,85	0	25	6,78	15,39	0	49
Bonusprogramm (z. B. Payback)	15,44	27,14	0	87	4,78	8,79	0	24
EV-SSL-Zertifikat	64	33,48	0	100	52,11	37,46	0	100
Expertenbeurteilungen, Testberichte, Preise	44	33,06	0	90	30,89	28,7	0	79
FAQ bzw. Hilfesektion	36,56	26,18	0	66	30,67	30,66	0	87
Firmeninformationen (Wir über uns)	38,78	30,88	0	88	37,33	29,47	0	80

Hinweis	Kurzer Blick			Langer Blick				
	$\bar{x}$	(s)		$\bar{x}$	(s)		$\bar{x}$	(s)
Garantien	36,56	27,06	0	82	34,22	33,3	0	95
Gewerberegister und –nummer	34,22	34,97	0	89	21	33,98	0	94
Großes Artikelsortiment	16,44	27,48	0	90	15,11	27,77	0	89
Gütesiegel	47,33	24,55	12	80	38,11	27,02	0	83
Hinweis auf Rückgaberechte	30,78	24,99	0	76	18,67	21,59	0	63
Hinweis MwSt., bzw. USt.	19,89	19,04	0	51	10,56	18,65	0	58
https in URL	68,33	29,77	0	97	46,67	34,74	0	100
Individuelle Accounts/Benutzer Log-Ins	31,33	26,72	0	72	20,44	26,27	0	80
Informationen zum Datenschutz, -sicherheit	42,78	37,31	0	95	62,11	39,08	0	100
Informationen zur Kontaktaufnahme	43,33	25,14	13	77	27,89	31,66	0	79
Internetbezahlsysteme (z. B. Paypal)	29,33	32,39	0	82	23,22	34,18	0	89
Klare Preisangabe	51,78	40,82	0	100	34,11	41,99	0	94
Kundenbeurteilungen des Shops	57,44	29,92	1	100	51,33	30,64	0	87
Links zu verwandten Websites	23,78	23,99	0	64	10,22	14,89	0	36
Look-in-Feature	24,44	22,65	0	57	6,33	12,04	0	33
Name und Anschrift des Anbieters	64,56	29,09	8	100	56	31,81	0	100
Produktbeschreibung	38,33	35,68	0	92	27,33	36,2	0	90
Produktbild	33,89	30,5	0	79	26,67	29,91	0	92
Produktempfehlungen	17	17,04	0	47	15,22	19,53	0	56
RSS-Feed	5,89	8,87	0	24	1,11	3,14	0	10
Shopname (URL)	39,22	29,97	0	86	22,67	28,59	0	77
Social Bookmarks	15,44	26,57	0	84	2,56	4,55	0	12
Sprachoptionen	12	15,25	0	47	3	5,85	0	17
Umsatzsteuer-Identifikationsnummer	34,89	27,83	0	97	18,22	22,29	0	72
Unternehmensname und Rechtsformzusatz	52,44	34,02	0	89	32,78	30,54	0	83
Verfügbarkeitsanzeige	31,44	31,11	0	87	17,44	33,08	0	90
Verschiedene Versandoptionen	27,56	28,86	0	80	22,67	29,51	0	68
Viele Zahlungsmethoden	39,11	33,67	0	100	34,33	36,21	0	95

Sowohl bezüglich des kurzen Blickes als auch der eingehenderen Beschäftigung stellten *Name und Anschrift des Anbieters* (Mittelwerte 64,56, bzw. 56) und *EV-SSL Zertifikat* (Mittelwerte 64, bzw. 52,11) den zweit- bzw. drittwichtigsten Hinweis dar.
Als unwichtigste Hinweise ergaben sich bezüglich des kurzen Blickes *Besucherzähler* (Mittelwert 3,67) und bezüglich der eingehenderen Betrachtung *RSS-Feed* (Mittelwert 1,11).

3.2.2.2 Ranking der wichtigsten Hinweise auf den Umgang mit personenbezogenen Daten

Für Nutzer bedeutet es einen hohen Aufwand, sich bezüglich jedem dieser Hinweise ein Bild zu machen, bevor die persönlichen Daten angegeben werden. Aus dem Grund wurden die beteiligten Experten im Rahmen der Gewichtungsstudie weiterhin gefragt, welche der Hinweise auf den Umgang mit personenbezogenen Daten sie für die wichtigsten halten. Diese sollten von ihnen zusätzlich in eine Rangreihe gebracht werden.

Für jeden der hierbei genannten Hinweise wird im Weiteren ein zusammenfassender Wert ermittelt. Da maximal fünf Hinweise genannt werden sollten, werden jedem Hinweis, der von einem Experten als wichtigster eingeordnet wurde, fünf Punkte zugeordnet. Der zweitwichtigste Hinweis entspricht im weiteren Verlauf entsprechend vier Punkten, der drittwichtigste drei usw. Im Anschluss wird für jeden der Hinweise über alle Experten eine Summe gebildet und die Hinweise nach dieser Summe in eine zusammenfassende Rangreihe gebracht (siehe Tabelle 5). Wie von Bortz erwähnt (2005) führt dieses Vorgehen dazu, dass dem Objekt mit der größeren Merkmalsausprägung eine größere Zahl zugeordnet wird und eine Ordinalskala entsteht. Zusätzlich wurde für jeden der Hinweise die Häufigkeit notiert, in welcher der jeweilige Hinweis als einer der wichtigsten Hinweise genannt wurde (Anzahl Nennungen).

Tabelle 5. Zusammenfassende Rangreihe der wichtigsten Hinweise auf den Umgang mit personenbezogenen Daten.

Hinweis	**Punkte Ranking**	**Anzahl Nennungen**
Informationen zu Datenschutz/Datensicherheit	32	8
EV-SSL-Zertifikat	19	6
Name & Anschrift des Anbieters	15	4
https in URL	14	5
Gütesiegel	10	4
Shopname (URL)	9	4
Expertenbeurteilungen, Testberichte…	9	3
Kundenbeurteilungen des Shops	7	3
Unternehmensname & Rechtsformzusatz	4	1
Internetbezahlsysteme (z. B. Paypal)	4	1
Individuelle Accounts/Benutzer Log-Ins	3	1
Firmeninformationen (Wir über uns)	3	1
USt-IdNr.	2	1
AGB	2	1
FAQ bzw. Hilfesektion	1	1
Bonusprogramm (z. B. Payback)	1	1

Es ergeben sich 16 Hinweise, die von mindestens einem Experten als einer der wichtigsten fünf Hinweise gewählt wurde. Die meisten Nennungen und auch die höchste Gesamtpunktzahl erreichte dabei *Informationen zu Datenschutz/Datensicherheit*. Entsprechend der Ergebnisse bezüglich der Wichtigkeiten belegen die Hinweise *EV-SSl-Zertifikat* und *Name und Anschrift des Anbieters* die folgenden Rangplätze. Sie tun dies allerdings in umgekehrter Reihenfolge. Auf den darauffolgenden Rängen liegen *https in URL*, *Gütesiegel*, *Shopname (URL)*, *Expertenbeurteilungen, Testberichte…* und *Kundenbeurteilungen des Shops*. Die Hinweise *Unternehmensname und Rechtsformzusatz*, *Internetbezahlsysteme*, *Individuelle Accounts/Benutzer Log-Ins*, *Firmeninformationen*, *USt-IdNr.*, *AGB*, *FAQ bzw. Hilfesektion* und *Bonusprogramm* werden jeweils nur einmal genannt.

3.2.2.3 Ergebnisse bezüglich der Quantifizierung von Datenschutz-Verhalten

Um im nächsten Schritt das beobachtete Verhalten in Zahlen ausdrücken zu können, werden die Beobachtungsdaten mit denen der Gewichtungsstudie in Zusammenhang gebracht. Ziel ist es, das von den Probanden gezeigte Verhalten mit Hilfe der Gewichtungsstudie einzuordnen. Als zentrales Ergebnis der Gewichtungsstudie werden die Einschätzungen der Wichtigkeit für einen kurzen Blick, bzw. eine

darüberhinausgehende Beschäftigung bezüglich der wichtigsten Hinweise angesehen. Die Rangreihe der wichtigsten Hinweise ist in Tabelle 5 dargestellt. Da nicht alle Hinweise von allen Experten genannt wurden und somit die Punktzahlen nicht immer auf der gleichen Anzahl von Bewertungen beruhen, wird darauf verzichtet, die Abstände in der Rangreihe weiter zu berücksichtigen. Darüber hinaus werden die Hinweise, die nur von einem Experten als einer der fünf wichtigsten Hinweise genannt wurden, für das weitere Vorgehen ausgeschlossen. Es ergeben sich daraus insgesamt 8 wichtigste Hinweise, die in Tabelle 6 mit dem dazugehörigen arithmetischen Mittel bezüglich der Wichtigkeit ihrer Betrachtung dargestellt sind.

Tabelle 6. Mittelwerte (Skala von „unwichtig“ (0) bis „wichtig“ (100)) der acht wichtigsten Hinweise nach dem Ranking im Rahmen der Gewichtungsstudie.

Hinweis	**Kurzer**	**Langer Blick**
	Mittelwert	**Mittelwert**
Informationen zu Datenschutz/Datensicherheit	42,78	62,11
EV-SSL-Zertifikat	64,00	52,11
Name & Anschrift des Anbieters	64,56	56,00
https in URL	68,33	46,67
Gütesiegel	47,33	38,11
Shopname (URL)	39,22	22,67
Expertenbeurteilungen, Testberichte…	44,00	30,89
Kundenbeurteilungen des Shops	57,44	51,33

Im ersten Schritt soll nun überprüft werden, ob sich die errechneten Mittelwerte der Wichtigkeiten der acht Hinweise signifikant voneinander unterscheiden oder ob alle Hinweise als gleich wichtig angesehen werden müssen. Um diese Frage beantworten zu können, verwendet man die Methode der Varianzanalyse mit Messwiederholung. Von Messwiederholung spricht man dann, wenn verschiedene gemessene oder erfragte Werte von den gleichen Personen, also der gleichen Stichprobe stammen (Eid, Gollwitzer & Schmitt, 2010).

Als Voraussetzungen für eine Varianzanalyse mit Messwiederholung werden folgende Annahmen angegeben:

1. Die Messungen sind voneinander abhängig.
2. Die abhängige Variable ist mindestens intervallskaliert.
3. Der Innersubjektfaktor ist nominalskaliert.
4. Die abhängige Variable sollte (möglichst) für jede Stufe des Innersubjektfaktors normalverteilt sein.
5. Es liegen keine Ausreißer in den Daten vor.
6. Sphärizität ist gegeben.

Wie bereits erwähnt stammen alle Angaben, die verglichen werden sollen, von derselben Stichprobe, wodurch die erste Voraussetzung erfüllt ist. Die abhängige Variable stellt in diesem Fall die eingeschätzte Wichtigkeit dar, die aufgrund der Nutzung der kontinuierlichen Skala mit Werten von 0-100 mindestens intervallskaliert vorliegt. Als Innersubjektfaktor werden die acht Einschätzungen der Hinweise

verwendet. Die Unterteilung in acht „Kategorien“ entspricht einer Nominalskalierung. Die Voraussetzungen, welche die Skalierung der Daten betreffen, sind demnach auch erfüllt. Die restlichen drei Voraussetzungen werden mit Hilfe der SPSS Software geprüft. Um das Vorliegen einer Normalverteilung testen zu können, verwendet man in diesem Rahmen entweder den sogenannten Kolmogorov-Smirnov-Test oder den Shapiro-Wilk-Test. Beide Tests testen die Nullhypothese, dass die Daten normalverteilt sind (Razali & Wah, 2011). Ein signifikantes Ergebnis führt zur Ablehnung dieser Nullhypothese (Eid et al., 2010). Da der Shapiro-Wilk-Test über mehr statistische Power verfügt, ist er dem Kolmogorov-Smirnov-Test vorzuziehen (Razali & Wah, 2011). Tabelle 7 zeigt die Ergebnisse der Untersuchung.

Tabelle 7. Ergebnisse des Shapiro-Wilk Tests auf Normalverteilung (p-Werte) der Variablen der eingeschätzten Wichtigkeit für eine kurze Überprüfung auf Vorhandensein des entsprechenden Hinweises.

Hinweis	**p-Wert**
Informationen zu Datenschutz/Datensicherheit	.118
EV-SSL-Zertifikat	.282
Name & Anschrift des Anbieters	.393
https in URL	.074
Gütesiegel	.260
Shopname (URL)	.306
Expertenbeurteilungen, Testberichte…	.338
Kundenbeurteilungen des Shops	.699

Es zeigt sich, dass bei allen acht Einschätzungen der Wichtigkeit der Überprüfung des Vorhandenseins mittels eines kurzen Blickes von einer Normalverteilung ausgegangen werden kann, da keiner der Tests zu einem signifikanten Ergebnis ($p<.05$) kam. Um im nächsten Schritt Ausreißer ermitteln zu können, wurden Boxplots erstellt. Die optische Überprüfung dieser zeigt, dass keine Ausreißer vorliegen. Die sogenannten Sphärizität liegt dann vor, wenn die Variablen, welche die Differenzen zwischen den, in diesem Falle 8 Messwerten abbilden (Differenzvariablen) die gleiche Varianz aufweisen (Eid et al., 2010).

Um die Sphärizität im letzten Schritt überprüfen zu können, wird im Rahmen von SPSS der Mauchly-Test auf Sphärizität verwendet (Eid et al., 2010). Bei einem signifikanten Ergebnis ($p<.05$) ist nicht davon auszugehen, dass Sphärizität gegeben ist. Der errechnete Wert liegt in diesem Falle bei $p=.082$, weshalb auch die letzte Voraussetzung zur Durchführung der ANOVA (analysis of variance) mit Messwiederholung als erfüllt gilt. Diese kam mit $F(7,56) = 1.805$, $p = .104$ zu keinem signifikanten Ergebnis. Die Einschätzungen der Wichtigkeit bezüglich der acht Hinweise unterscheiden sich demnach nicht signifikant. Die acht wichtigsten Hinweise werden deshalb im Folgenden als gleich wichtig angesehen.

Es stellt sich nun die Frage, ob es in Bezug auf einen der Hinweise wichtiger ist mit einem kurzen Blick zu überprüfen, ob der jeweilige Hinweis auf der Webseite vorhanden ist, oder ob der entsprechende Hinweis darüber hinaus in Augenschein genommen werden sollte. Um diese Frage beantworten zu können, werden die Mittelwerte beider Beurteilungen miteinander verglichen. Ein t-Test für abhängige Stichproben macht dann eine Aussage darüber, ob sich die beiden Mittelwerte signifikant voneinander unterscheiden. Voraussetzung für diesen Test ist es, insbesondere bei kleinen Stichproben (n = Anzahl der Messwertpaare <30), dass die Differenzen in der Stichprobe annähernd normalverteilt sind (Bortz,

2005). Tabelle 8 zeigt die Ergebnisse der Tests auf Normalverteilung bezüglich der Wichtigkeit der eingehenderen Betrachtung der Hinweise.

Tabelle 8. Ergebnisse des Shapiro-Wilk Tests auf Normalverteilung (p-Werte) der Variablen der eingeschätzten Wichtigkeit für eine eingehendere Betrachtung des entsprechenden Hinweises.

Hinweis	**p-Wert**
Informationen zu Datenschutz/Datensicherheit	.021
EV-SSL-Zertifikat	.198
Name & Anschrift des Anbieters	.716
https in URL	.320
Gütesiegel	.749
Shopname (URL)	.010
Expertenbeurteilungen, Testberichte...	.171
Kundenbeurteilungen des Shops	.192

Es zeigt sich, dass bei allen Variablen, außer bei der Einschätzung der Wichtigkeit einer eingehenderen Betrachtung von *Informationen zum Datenschutz/Datensicherheit* und des *Shopname (URL),* von einer Normalverteilung auszugehen ist. Zwar reagiert der t-Test für abhängige Stichproben relativ robust auf Verletzungen der Voraussetzung der Normalverteilung, jedoch sollte in diesem Fall überprüft werden, ob eine positive Korrelation des Messwertpaares vorliegt (Bortz, 2005). Im Falle der Variablen *Informationen zum Datenschutz/Datensicherheit* und *Shopname (URL)* korrelieren die Einschätzungen der Wichtigkeit eines kurzen Blickes und der eingehenderen Betrachtung nicht signifikant miteinander (*Informationen zum Datenschutz/Datensicherheit* $p=.731$; *Shopname (URL)* $p=.192$). In diesem Fall wird empfohlen, statt des t-Tests auf den sogenannten Wilcoxon-Test zurückzugreifen (Bortz, 2005). Dieser geht von der Nullhypothese aus, dass sich die Messwerte nicht unterscheiden. Aufgrund einer Wahrscheinlichkeit von $p=.327$ im Falle der *Informationen zum Datenschutz/Datensicherheit* und $p=.173$ im Falle der Variable *Shopname (URL)* werden diese Nullhypothesen beibehalten. Für die anderen sechs Messwertpaarungen, welche die Voraussetzung der Normalverteilung nicht verletzen, konnte jeweils ein t-Test für abhängige Stichproben berechnet werden. Bei diesem wird die Nullhypothese untersucht, dass die durchschnittliche Differenz zwischen den Messwerten 0 entspricht (Bortz, 2005). Wie in Tabelle 9 abgebildet zeigt der Test in keinem der Fälle ein signifikantes Ergebnis. Die Nullhypothese kann somit in keinem der Fälle verworfen werden.

Inhaltlich bedeutet das, dass in Bezug auf keinen der acht wichtigsten Hinweise ein Unterschied in der Wichtigkeit für einen kurzen Blick und der Wichtigkeit für eine eingehendere Beschäftigung mit diesem Hinweis besteht. Eine Unterscheidung, ob ein Hinweis nur kurz oder länger betrachtet wurde, ist demnach überflüssig. Im weiteren Vorgehen wird deshalb nur überprüft, ob ein Proband/eine Probandin einen entsprechenden Hinweis fixiert hat oder nicht. Die Summe der positiven Bewertungen dieser dichotomen Antwortmöglichkeiten steht dann stellvertretend für das gezeigte Datenschutz-Verhalten. Dieses Vorgehen entspricht dem sogenannten ungewichteten additiven Index, wie er von Döring (2016) beschrieben wird.

Dabei ist es irrelevant, ob alle acht Hinweise auf der jeweiligen Webseite überhaupt zu finden waren. Denn als sicherstes Verhalten wird die Überprüfung des Vorhandenseins aller acht wichtigsten Hinweise angesehen. Die Akzeptanz des Fehlens eines dieser Hinweise wird mit der fehlenden Überprüfung des Vorhandenseins gleichgesetzt.

Tabelle 9. Ergebnis des t-tests für abhängige Stichproben.

Hinweis (-paar)	df	p-Wert
Informationen zu Datenschutz/Datensicherheit	8	.370
EV-SSL-Zertifikat	8	.516
Name & Anschrift des Anbieters	8	.492
https in URL	8	.222
Gütesiegel	8	.337
Shopname (URL)	8	.187
Expertenbeurteilungen, Testberichte...	8	.240
Kundenbeurteilungen des Shops	8	.707

3.2.3 Diskussion Gewichtungsstudie

Für die durchgeführte Gewichtungsstudie wurde sich für die Methode einer Online-Befragung entschieden. Diese Art der Erhebung bietet sowohl Vorteile als auch Nachteile. Einer der Vorteile ist, dass es sich um eine sehr günstige Methode handelt, da ein in diesem Falle kostenloses Tool verwendet werden konnte, was zu Einsparungen an Material und Personalkapazitäten führt (Hewson, Laurent & Vogel, 1996). Einen zusätzlichen Vorteil stellt die Tatsache dar, dass eine online Befragung von den Teilnehmern zu jedem Zeitpunkt ausgefüllt werden kann, der zeitlich am besten passt (Huber, 2005). Dies wurde insbesondere im Rahmen der hier vorliegenden schwer erreichbaren Zielgruppe der Experten aufgrund deren häufig sehr eingeschränkten Zeit (Döring & Bortz, 2016) als Vorteil gesehen. Darüber hinaus ist es möglich, den Fragebogen weiter zu streuen und so auch Personen zu erreichen, die man unter anderen Umständen nicht erreichen würde (Gosling, Vazire, Srivastava & John, 2004). So konnten 9 Experten für die Teilnahme an der Studie gewonnen werden. Diese Anzahl an Experteneinschätzungen wird, angelehnt an Demeter (2015) als ausreichend angesehen.
Die befragten Experten nähern sich dem Thema „Datenschutz beim Onlineshopping“ mit unterschiedlichen Hintergründen. Diese Tatsache wird als wichtig angesehen, um zu ermöglichen, dass die jeweilige Wichtigkeit der Hinweise umfassend beurteilt wurde. Die angegebenen aktuellen Berufsbezeichnungen sowie eine Beschäftigung mit der zu bewertenden Thematik von mindestens 2 Jahren werden als ausreichende Qualifikation im Rahmen dieser Expertenbefragung angesehen. Die Aufgabe der Experten bestand darin, zunächst die Wichtigkeit einzuschätzen mit einem kurzen Blick zu überprüfen, ob ein Hinweis auf der jeweiligen Webseite vorhanden ist und auf der gleichen Skala die Wichtigkeit einer darüber hinaus gehenden Überprüfung des Hinweises anzugeben. Im nächsten Schritt sollten die fünf wichtigsten Hinweise genannt und in eine Reihenfolge gebracht werden. Am Ende der Befragung hatten die Experten die Möglichkeit in einem freien Feld jegliche Art von Rückmeldung zu geben. Als kritisch wurde im Vorfeld der Befragung die gleichzeitige Einschätzung sowohl der Wichtigkeit einer kurzen Überprüfung als auch einer darüberhinausgehenden Betrachtung auf einer gemeinsamen Skala angesehen. Generell bietet die verwendete visuelle Analogskala eine Erfassung eines Merkmals unter Verzicht der Angabe häufig strittiger Merkmalsabstufungen (Döring & Bortz, 2016). Darüber hinaus wird angenommen, dass die beiden Icons (Auge und Leselupe), die verwendet wurden, um die beiden Regler zu markieren, diese gut und leicht verständlich voneinander abgrenzbar machten.

Doch gaben zwei der Experten an, dass sie mit der Art der Einschätzung ihre Probleme hatten. Als Vorteil wurde es im Vorfeld gesehen, dass diese Art der Abfrage den direkten Vergleich beider Einschätzungen ermöglichte. Es wird darüber hinaus davon ausgegangen, dass der dadurch verringerte Eindruck des benötigten Aufwandes dazu beigetragen hat, dass es zu keinen Abbrüchen während des Ausfüllens des Fragebogens kam. Die einfache Möglichkeit, eine bereits gestartete Befragung abzubrechen, stellt einen der Nachteile der gewählten Methode der Online-Befragung dar (Huber, 2005). Ein weiterer Nachteil ist der, dass nicht mit absoluter Sicherheit davon ausgegangen werden kann, dass alle verwendeten Begriffe und Darstellungen von allen Probanden gleich verstanden wurden (Kraut et al., 2004). Drei von ihnen beschrieben im Rahmen ihrer Rückmeldung ihre Schwierigkeiten in Bezug auf die Interpretation einzelner Items. Zwei von diesen dreien gaben hierzu aber an, dass sie die jeweiligen, mehrfach interpretierbaren Items mit „Datenschutz“, bzw. „Sicherheit“ in Bezug setzten. Dies entspricht dem gewünschten Vorgehen.
Erwähnenswert ist die teilweise sehr große Uneinigkeit der Einschätzungen der Experten. Es wurde vermutet, dass diese ihren Grund in der Annäherung an das Thema aus verschiedenen fachlichen Kontexten hat. Trotz der auffälligen Unterschiede in der Einschätzung der Wichtigkeiten konnten augenscheinlich aber zunächst keine systematischen Zusammenhänge zwischen diesen und den thematischen Hintergründen festgestellt werden. Die Reduzierung der evaluierten 40 Hinweise auf die acht wichtigsten ergab sich aus den durchgeführten Expertenrankings.
Bei genauerer Betrachtung zeigten sich hier Unterschiede, die sich durch die unterschiedlichen thematischen Hintergründe begründen lassen. So wurden nur drei (*Informationen zu Datenschutz/Datensicherheit, https in URL* & *EV-SSL-Zertifikat*) der acht wichtigsten Hinweise von Experten aus allen Richtungen unter die wichtigsten gewählt. Bei genauer Betrachtung der eingeschätzten Wichtigkeiten zeigt sich, dass insbesondere die Experten mit technischem Hintergrund und die Experten mit juristischem Hintergrund sich uneinig sind. Während die Tendenz bei den Experten mit technischem Hintergrund zu eingehenderer Beschäftigung mit diesen drei Hinweisen führt, tendieren die Experten mit juristischem Backround zur kurzen Betrachtung. Zusätzlich auffällig zeigen sich die Daten bezüglich des Hinweises *Name & Anschrift des Anbieters*. Dieser wurde von allen Juristen als einer der fünf wichtigsten genannt, aber von keinem Experten, der sich aus einem anderen Kontext heraus dem Thema nähert. Insgesamt wird diese Uneinigkeit als gewinnbringend angesehen, da die erhaltenen acht wichtigsten Hinweise somit die unterschiedlichen Aspekte des Datenschutzes berücksichtigt.
Eine Gewichtung der acht Hinweise ergab sich, vermutlich teilweise auch begründet mit diesen Uneinigkeiten, nicht. Darüber hinaus konnten auch keine Unterschiede bezüglich der notwendigen Dauer der Beschäftigung mit dem jeweiligen Hinweis festgestellt werden.

3.3 Anforderungen an die Erhebung

Die in Kapitel 2.4.3 vorgestellten Methoden zur Erfassung von tatsächlichem Datenschutz-Verhalten geben gute Hinweise auf Anforderungen, die an eine solche Erhebung gestellt werden müssen. Die wichtigste ergibt sich hierbei aus der Tatsache, dass das Setting, in dem sich die Probanden während der Erhebung befinden, dem entsprechenden Kontext entspricht. Da im Rahmen dieser Arbeit Datenschutz-Verhalten beim Onlineshopping untersucht werden soll, müssen sich die Teilnehmer notwendigerweise im Kontext des Onlineshoppings wiederfinden. Das von ihnen gezeigte Verhalten soll dabei möglichst dem tatsächlichen Verhalten in der jeweiligen Situation entsprechen. In Kapitel 3.1 wurde bereits herausgearbeitet, dass es sich bei dem zu beobachtenden Verhalten um die Überprüfung, der auf den

Seiten eines Webshops angegebenen Hinweise auf den Umgang mit personenbezogenen Daten handeln soll. Diese Überprüfung findet auf den Seiten eines Anbieters, bei dem in der Vergangenheit bereits Produkte bestellt wurden, möglicherweise weniger ausgeprägt statt. Kim et al. (2012) begründen das damit, dass die Unsicherheit und das wahrgenommene Risiko bei potentiellen Kunden höher ist, als das von Wiederkäufern. Aus dem Grund soll die gestellte Aufgabe gewährleisten, dass die Teilnehmer sich auf den Seiten eines Webshops orientieren müssen, der ihnen nicht bereits in der Form bekannt ist. Bezugnehmend auf die bei Tsai et al. (2011) festgestellte Einschränkung, dass dort die zu kaufenden Produkte vorgegeben wurden, sollen die Teilnehmer im Rahmen dieser Erhebung möglichst frei wählen können, welches Produkt sie erwerben möchten. Whalen und Inkpen (2005) erwähnen als Einschränkung bezüglich der von ihnen durchgeführten Studie, dass ihre Probanden nicht die eigenen Daten verwendeten. Darüber hinaus konnten Schechter et al. (2007) nachweisen, dass sich das Verhalten der Teilnehmer, die ihre eigenen Daten in Gefahr sahen, von denen unterschied, die fremde, bzw. fiktive Daten verwendeten. Für den Kauf im Rahmen dieser Erhebung sollen deshalb jeweils die eigenen, persönlichen Daten verwendet werden. Durch den Kauf, selbst gewählter Produkte mit den eigenen Daten soll zusätzlich eine Situation geschaffen werden, die den Fokus der Teilnehmer nicht ausschließlich auf die Aufgabenerfüllung lenkt, wie Whalen und Inkpen (2005), Schechter et al. (2007) und Egelman et al. (2008) in Bezug auf ihre Studien kritisierten.
Trotzdem soll die, an die Teilnehmer gestellte Aufgabe sie möglichst von der Beobachtungssituation und dem sich dadurch ergebenden Grad an Künstlichkeit ablenken, da auch dies sonst zu Verfälschungen des gezeigten Verhaltens führen kann (Döring & Bortz, 2016). Laut Schechter et al. (2007) wird von Forschern diskutiert, ob es möglich ist, im Versuch eine reale Erfahrung des Angegriffen-werdens zu erschaffen, die mit den ethischen Standards konform geht. Die Autoren kommen dabei zu dem Schluss, dass die Teilnehmer nur soweit „getäuscht“ werden müssen, dass sie sich weniger sicher fühlen, als sie das eigentlich sind. Im Rahmen dieser Studie soll auch dies durch die Verwendung der eigenen Daten gegeben sein. Die Sicherheit bezüglich der Daten der Teilnehmer soll dadurch gewährleistet werden, dass in dem Moment, in dem eine Dateneingabe erfolgen soll, der Versuch vom jeweiligen Versuchsleiter/Versuchsleiterin abgebrochen wird.
Um ein gewisses Maß an Standardisierung zu bieten, wird die Instruktion der Aufgabe den Teilnehmern schriftlich vorgelegt, und ihnen ausreichend Zeit zum Lesen, bzw. für Rückfragen gegeben werden. Um diese schon möglichst zu vermeiden, muss die Instruktion kurz, klar und verständlich formuliert sein (Huber, 2005). Darüber hinaus soll generell eine Situation geschaffen werden, die dazu führt, dass die Teilnehmer der Studie sich möglichst wohl fühlen und frei von Unsicherheiten und Ängsten sind, da auch dies Störvariablen im Rahmen eines Versuches darstellen (Huber, 2005). Neben wohltemperierten, störungsfreien Räumlichkeiten gehört hierzu unter anderem, dass die Teilnehmer höflich behandelt und im Rahmen des Möglichen über die Inhalte der Studie aufgeklärt werden (Huber, 2005). Dabei ist es nicht notwendig, dass sie gleich nachvollziehen können, wie die zugrundeliegenden Hypothesen geartet sind. Dies könnte sogar störend wirken, weil die Probanden ihr Verhalten daran anpassen könnten (Huber, 2005). Um trotzdem Unsicherheiten abzubauen, sollen die Teilnehmer im Rahmen dieser Erhebung darüber aufgeklärt werden, dass die Daten anonymisiert erfasst und nicht weitergegeben werden. Zusätzlich soll erwähnt werden, dass nicht ihre Leistung analysiert wird und nicht ihre Daten als einzelne Person für Aussagen verwendet werden, sondern dass generell interessiert, wie Menschen sich verhalten. Deshalb solle man sich möglichst normal verhalten. Hierfür ist es notwendig, dass die teilnehmenden Probanden bereits über Erfahrungen in Bezug auf Online-shopping verfügen.
Um bei der Datenerhebung möglichst standardisiert vorgehen zu können, soll diese neben Fragebögen mit Hilfe eines Eye-Trackers durchgeführt werden. Daraus ergibt sich die Notwendigkeit von Einzelversuchen, statt der Erhebung einer ganzen Gruppe zur gleichen Zeit. Laut Pfeiffer et al. (2013)

verspricht die Kombination aus Blickbewegungsdaten mit der qualitativen oder quantitativen Messungen von Entscheidungsstrategien oder Einflussfaktoren Einsichten in das Verhalten im Umgang mit einem potentiellen Risiko. Helmert et al. (2017) geben an, dass die Orientierung an den Augen eine direkte Messung der visuellen Aufmerksamkeit ermöglicht, während Fragebögen und Befragungen oftmals Verzerrungen unterliegen.
Durch den Einsatz der Methode der Blickbewegungsanalyse lässt sich die von Whalen und Inkpen (2005), Schechter et al. (2007) und Norberg et al. (2007) in Bezug auf ihre Studien erwähnte Einschränkung der Laborumgebung, bzw. des universitären Umfelds, welche Probanden eine gewisse Sicherheit vermittelt, nicht umgehen. Genauso lässt sich die in diesem Kontext ebenso relevante Einverständniserklärung, die Schechter et al. (2007) erwähnen, unter ethischen und rechtlichen Gesichtspunkten nicht vermeiden. Bezugnehmend auf ihre kritische Betrachtung der von Norberg et al. (2007), Tsai et al. (2011) und Beresford et al. (2012) verwendeten Stichproben, soll im Rahmen dieser Studie eine Stichprobe verwendet werden, die bezüglich der demographischen Merkmale möglichst breit gestreut ist. Dies schließt die Einbeziehung von ausschließlich studentischen Teilnehmern aus. In Bezug auf finanzielle und zeitliche Ressourcen ist es notwendig, die Stichprobengröße auf maximal 50 Teilnehmer zu begrenzen. Laut Döring und Bortz (2016) gelten aber kleine und nicht-zufällige Stichproben für explorative Studien als ausreichend.

Fazit

Um Aussagen über das tatsächliche Datenschutz-Verhalten beim Onlineshopping machen zu können, wird demnach, für 50 Teilnehmer einer Studie, mittels Blickbewegungsanalyse überprüft, ob bzw. welche im Rahmen der Gewichtungsstudie als wichtigste identifizierte Hinweise bezüglich der Vertrauenswürdigkeit eines Webshops betrachtet werden. Damit wird *Forschungsfrage 1a: Wie kann tatsächliches Datenschutz-Verhalten beim Onlineshopping operationalisiert werden?* beantwortet. Als Maß wird hierfür die Größe der Fixation verwendet. Diese wird als das Verweilen des Blickes in einem Umkreis von weniger als 2° Sehwinkel (bzw. 87 px) für eine Dauer von mindestens 100 ms definiert. Darüber hinaus werden Fixationsdauern von 100-200 ms als *kurzer Blick* und Fixationsdauern von >200 ms als *eingehendere Betrachtung* definiert. Im Rahmen der Gewichtungsstudie ergaben sich allerdings keine Unterschiede bezüglich der Wichtigkeit dieser beiden Kategorien. Die Summe der, von den acht wichtigsten Hinweisen tatsächlich betrachteten Hinweise gilt deshalb als Maß für das tatsächliche Datenschutz-Verhalten beim Onlineshopping. *Forschungsfrage 1b: Wie kann erhobenes Verhalten für weitere Analysen quantifiziert werden?* gilt diesbezüglich als beantwortet. Bei der Gestaltung der benötigten Studie werden die gesammelten Anforderungen, wie das Schaffen einer möglichst realistischen Situation, der weitestgehenden Standardisierung der Erhebung und das Erheben einer, bezüglich der demographischen Attribute möglichst breit aufgestellten Stichprobe, beachtet werden. Die gesammelten Anforderungen beantworten dementsprechend *Forschungsfrage 1c: Welche Anforderungen bestehen an eine solche empirische Erhebung?*

4 Ermittlung potentieller personenbezogenen Prädiktoren

Im Anschluss an die Erarbeitung einer Möglichkeit, tatsächliches Datenschutz-Verhalten beim Onlineshopping zu erfassen und der Sammlung von Anforderungen an eine entsprechende Studie, folgt in diesem Kapitel die Beschreibung ebendieser. Ziel der Studie ist neben der Erfassung des tatsächlichen Verhaltens die Ermittlung potentieller Prädiktoren auf dieses Verhalten. Im Zuge dessen wird zunächst basierend auf den in Kapitel 2.4.1 dargestellten Theorien, Modellen und Erkenntnissen ein Arbeitsmodell aufgestellt, welches sich zur Ableitung entsprechender Hypothesen eignet. Das Arbeitsmodell und die Hypothesen sind in Kapitel 4.1 dargestellt. Im Anschluss wird das Vorgehen im Rahmen dieser ersten Explorationsstudie (Kapitel 4.2) und deren Ergebnisse (Kapitel 4.3) beschrieben. Die Ergebnisse bezüglich der Hypothesentests sind in Kapitel 4.4 dargestellt. Den Abschluss des Kapitels stellt die Diskussion bezüglich der durchgeführten Explorationsstudie dar (Kapitel 4.5).

4.1 Ableitung des Arbeitsmodells und Hypothesen

Wie bereits in Kapitel 2.4.1 beschrieben sind die dort dargestellten Erkenntnisse sehr umfassend im Modell von Pfeiffer et al. (2013) dargestellt. Dieses Modell stellt die potentiellen Faktoren dar, die einen Einfluss darauf haben, ob eine beliebige Person dem Aufruf im Rahmen einer beliebigen Email folgt, einen darin enthaltenen Link anzuklicken. Es wird davon ausgegangen, dass sich dieser Kontext auf den Kontext von Webseiten übertragen lässt, da Studien, die sowohl Webseiten als auch E-mails als Stimuli verwendeten (Kumaraguru et al., 2007; Tsow & Jakobsson, 2007) ähnliche Effekte für beides fanden (Pfeiffer et al., 2013). Trotzdem bedarf das Modell in der vorgestellten Version diesbezüglich einiger Anpassungen.

Das tatsächliche Verhalten, welches im Ausgangsmodell von Pfeiffer et al. (2013) das Öffnen des Emailanhanges darstellt, wird im Rahmen des hier zu erarbeitenden Modells durch das *tatsächliche Datenschutz-Verhalten im Rahmen von Onlineshopping* ersetzt. Entsprechend der Theorie des überlegten Handelns (Fishbein & Ajzen, 1975) und der Theorie des geplanten Verhaltens (Ajzen, 1985) geht diesem Verhalten eine Intention für selbiges voraus. Die Intention entspricht der subjektiven Wahrscheinlichkeit dafür, dass das gefragte Verhalten gezeigt wird, weshalb sie im Rahmen des Modells als *Wahrscheinlichkeit für Datenschutz-Verhalten im Rahmen von Onlineshopping* benannt wird. Diese Wahrscheinlichkeit wird entsprechend dem Modell von Pfeiffer et al. (2013) und darin einbezogenen Erkenntnissen (z. B. Blais & Weber, 2006; Hanoch et al., 2006; Weber et al., 2002) von einem *wahrgenommenen Risiko* und einem *erwarteten Nutzen* beeinflusst. Die beiden Faktoren sollen sich im Rahmen dieser Arbeit entsprechend der in Kapitel 2.4.1 vorgestellten Arbeiten zur Domain-Specific Risk-Taking Scale (Blais & Weber, 2006; Weber et al., 2002) auf ganz bestimmte risikobehaftete Handlungen beziehen. Hierfür wurden die drei Handlungen ausgewählt: *Etwas online zu kaufen, ohne vorher die AGB zu lesen, im Internet Daten anzugeben, ohne vorher die Datenschutzerklärungen angeschaut zu haben* und *vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt*.

Im Rahmen dieser Arbeit soll darüber hinaus die Einschränkung vorgenommen werden, die zu ermittelnden, potentiellen Einflussfaktoren möglichst auf diejenigen zu beschränken, die in der Person der Nutzer liegen und nicht aus dem Wechselspiel mit einer bestimmten Webseite bzw. eines Anbieters entstehen. Diese sind im Ausgangsmodell von Pfeiffer et al. (2013) als demographische Eigenschaften der Nutzer dargestellt. In Kapitel 2.4.1 wurden diesbezüglich eine Reihe potentieller Einflussfaktoren

beschrieben. Diese Einflussfaktoren gehen in das zu erarbeitende Modell entsprechend dem Modell von Pfeiffer et al. (2013) als demographische Eigenschaften der Nutzer ein und wirken potentiell auf das wahrgenommene Risiko. Persönlichkeitseigenschaften wie *Neigung anderen zu vertrauen* oder das *Ausmaß an Gehorsamkeit* sollen dagegen nicht einbezogen werden. Auch das *Vertrauen,* welches in dem Falle einem Webshop, bzw. einem Anbieter gegenüber erbracht wird, wird in dieses Modell nicht übernommen, da hierfür jeweils ein entsprechendes Gegenüber benötigt wird. Gleiches gilt für die *Authentizität der Email*, die *Eigenschaften des Senders* sowie des *Kontexts*, die deshalb nicht auf die Anwendung auf einen Webshop angepasst werden. Es bleibt das von Pfeiffer et al. (2013) eingeführte *Gefahrenbewusstsein*, welches sich aus Wissen über und der Erfahrung mit der Bedrohung und dem potentiellen Umgang damit zusammensetzt. Basierend auf den Erkenntnissen, die bezüglich des Wissens im Rahmen des Internets in Kapitel 2.1.7 dargestellt wurden, sollen im Rahmen dieser Arbeit die Konstrukte *wahrgenommenes Wissen* und *tatsächliches Wissen* verwendet werden. Zusammengenommen mit den Variablen *Nutzungsdauer* und *Nutzungshäufigkeit*, sowie dem *Besitz internetfähiger Geräte* sollen diese Konstrukte als Variablen-Gruppe *Interneterfahrung des Nutzers* in das Modell einbezogen werden. Die *Interneterfahrung des Nutzers* wirkt sich vermutlich auf die Wahrscheinlichkeit aus, mit der das Verhalten gezeigt wird. Die Konstrukte in diesem Arbeitsmodell sind damit vollzählig. Da aber basierend auf den Erkenntnissen bezüglich des Privacy Paradoxons vermutet wird, dass das tatsächliche Verhalten nicht vollständig über die Intention, bzw. in dem Fall die Wahrscheinlichkeit vermittelt wird, wird in diesem Modell explorativ von Verbindungen von allen Konstrukten auf das tatsächliche Verhalten ausgegangen. Das sich ergebende Arbeitsmodell ist unter Abbildung 8 abgebildet.

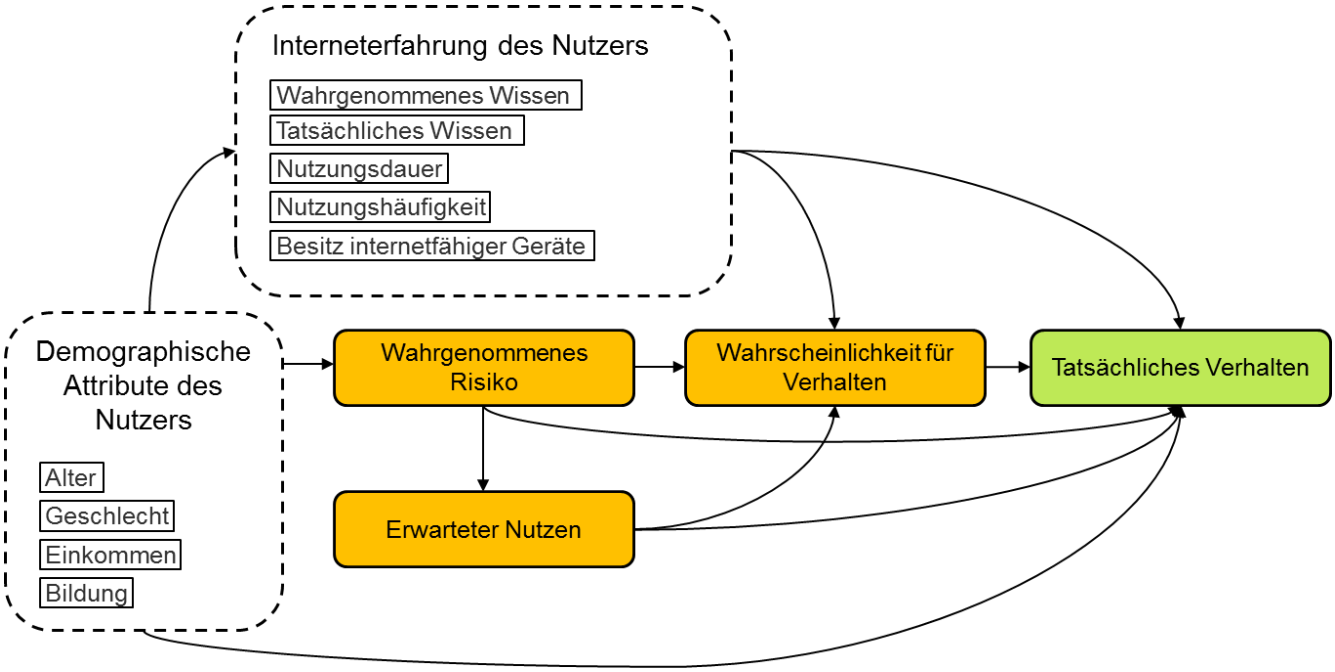


Abbildung 8. Aus, in Kapitel 2.4.1 dargestellten Erkenntnissen abgeleitetes Arbeitsmodell zur Vorhersage tatsächlichen Verhaltens.

Übereinstimmend mit den Erkenntnissen von Weber et al. (2002) enthält das Modell sowohl situations- als auch personenbasierte Komponenten. Weber et al. (2002) gehen davon aus, dass diese das Risikoverhalten hauptsächlich darüber beeinflussen, dass sie zu Unterschieden bezüglich der

Wahrnehmung des Risikos und des Nutzens führen und weniger zu Unterschieden bezüglich der Wahrscheinlichkeit für Verhalten.
Basierend auf dem Arbeitsmodell werden Hypothesen abgeleitet, die im Rahmen einer Explorationsstudie beantwortet werden sollen. Die Tatsache, dass der Fokus auf der Erfassung von tatsächlichem Verhalten liegen soll, bringt mit sich, dass die zu erwartende Stichprobengröße aufgrund unterschiedlicher Einschränkung wie monetärem und zeitlichem Aufwand zu gering sein wird, um das vorliegende Modell in Gänze zu testen. Es werden deshalb Hypothesen abgeleitet, die sich auf Unterschiede zwischen Gruppen beziehen und nicht auf Einflüsse zwischen Konstrukten, wie das im Rahmen einer Regression der Fall wäre. Die sich aus dem Arbeitsmodell ergebenden Hypothesen sind exemplarisch bezüglich der Variable Alter in Tabelle 10 zusammengefasst. Die Hypothesen bezüglich der anderen Variablen sind in Anhang D dieser Arbeit zu finden.

Tabelle 10. Hypothesen bezüglich der Variable *Alter*.

Hypothesen-kennzeichnung	**Hypothese**
Alter_1	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des tatsächlichen Wissens.
Alter_2	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des wahrgenommenen Wissens.
Alter_3	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich der Nutzungsdauer.
Alter_4	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich der Nutzungshäufigkeit.
Alter_5	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des Besitzes internetfähiger Geräte.
Alter_6	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des wahrgenommenen Risikos etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
Alter_7	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des wahrgenommenen Risikos im Internet Daten anzugeben, ohne die Datenschutz-erklärungen angeschaut zu haben.
Alter_8	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des wahrgenommenen Risikos vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
Alter_9	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des erwarteten Nutzens etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
Alter_10	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des erwarteten Nutzens im Internet Daten anzugeben, ohne die Datenschutz-erklärungen angeschaut zu haben.

Alter_11	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des erwarteten Nutzens vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
Alter_12	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich der Wahrscheinlichkeit etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
Alter_13	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich der Wahrscheinlichkeit im Internet Daten anzugeben, ohne die Datenschutzerklärungen angeschaut zu haben.
Alter_14	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich der Wahrscheinlichkeit vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
Alter_15	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich der tatsächlichen Handlung "etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen".
Alter_16	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich der tatsächlichen Handlung "im Internet Daten anzugeben, ohne die Datenschutz-erklärungen angeschaut zu haben".
Alter_17	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich der tatsächlichen Handlung "vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt".
Alter_18	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des tatsächlichen Datenschutz-Verhaltens.

Im Folgenden ist eine Explorationsstudie beschrieben, welche die empirische Erfassung des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping zum Ziel hat. Zusätzlich werden die Variablen des Arbeitsmodells erhoben, um die aufgestellten Hypothesen im Anschluss überprüfen zu können.

4.2 Explorationsstudie

Ziel dieser ersten explorativen Studie ist in erster Linie die empirische Erfassung des tatsächlichen Datenschutz-Verhaltens, basierend auf der in Kapitel 3.1 erarbeiteten Operationalisierung. Zusätzlich sollen dabei die unterschiedlichen Konstrukte des in Kapitel 4.1 aufgestellten Arbeitsmodells als Variablen erhoben werden. Kapitel 4.2 beschreibt das entsprechende Vorgehen im Rahmen der sogenannten Explorationsstudie und Kapitel 4.3 stellt deren Ergebnisse deskriptiv dar. Entsprechend des in Kapitel 3.2 erarbeiteten Verfahrens wird das aufgezeichnete Verhalten in quantitative Werte übersetzt. Diese ermöglichen Berechnungen, die zur Beantwortung der in Kapitel 4.1 aufgestellten Hypothesen führen. Die ersten Ergebnisse bezüglich des Arbeitsmodells sind in Kapitel 4.4 zusammengefasst. Das Vorgehen und die Ergebnisse der Explorationsstudie werden in Kapitel 4.5 diskutiert.

4.2.1 Vorgehen Explorationsstudie

Die Versuche im Rahmen der Explorationsstudie fanden im Zeitraum von 18. März bis zum 15. April 2013 in einem Raum des Institutes für Arbeitswissenschaft der Technischen Universität Darmstadt statt. Die teilnehmenden Probanden wurden vorwiegend im engeren und weiteren sozialen Umfeld der Versuchsleiterin und deren Betreuerin akquiriert. Hierfür wurden neben direkter Ansprache per Email verschiedene Verteiler in sozialen Netzwerken und entsprechenden Foren verwendet.

4.2.1.1 Versuchsaufbau

Der Raum war ausgestattet mit zwei gegenüberstehenden großen Schreibtischen und zwei Bürostühlen. Die Versuchsleiterin saß vor einem Monitor, der an einen feststehenden Tower-Rechner angeschlossen war und die Oberfläche der Software *SMI Experiment Center2™* zeigte. Mit Hilfe dieser Software wurde der gesamte Versuchsablauf koordiniert. Neben diesem Bildschirm stand ein Laptop PC der Firma Dell. Auf diesem wurden mit Hilfe der Software iView X™ die Blickbewegungen der Probanden aufgenommen. Laptop und Tower-Rechner waren mit Hilfe eines LAN-Kabels miteinander verbunden. Mit dem Tower-Rechner verbunden stand ein weiterer Monitor (22“ TFT) auf dem gegenüberliegenden Probandenarbeitsplatz. An dessen oberen Rand wurde eine Webcam befestigt. Sie filmte die Probanden während des gesamten Versuchs. Unterhalb des Bildschirms befand sich der RED remote eye tracker (60/120Hz) der Firma SMI. Die, für die Blickbewegungsaufzeichnung relevanten Stimuli, wurden mit einer Auflösung von 1680 px x 1050 px, bzw. physikalisch 474 mm x 297 mm dargestellt. Zur Blickerfassung war ein Abstand zwischen dem Kopf des Probanden und dem Monitor von 700 mm im System voreingestellt. Auf diesem Monitor wurden den Probanden auch alle Fragebögen dargeboten. Die Fragebögen wurden im Vorfeld als Online-Fragebogen mit Hilfe des Software-Pakets SoSci Survey (*SoSciSurvey.de,* o.D.) konzipiert. Auf Abbildung 9 ist der Arbeitsplatz der Versuchsleiterin und auf Abbildung 10 der Probandenarbeitsplatz, jeweils aus Sicht der jeweiligen Person, dargestellt.

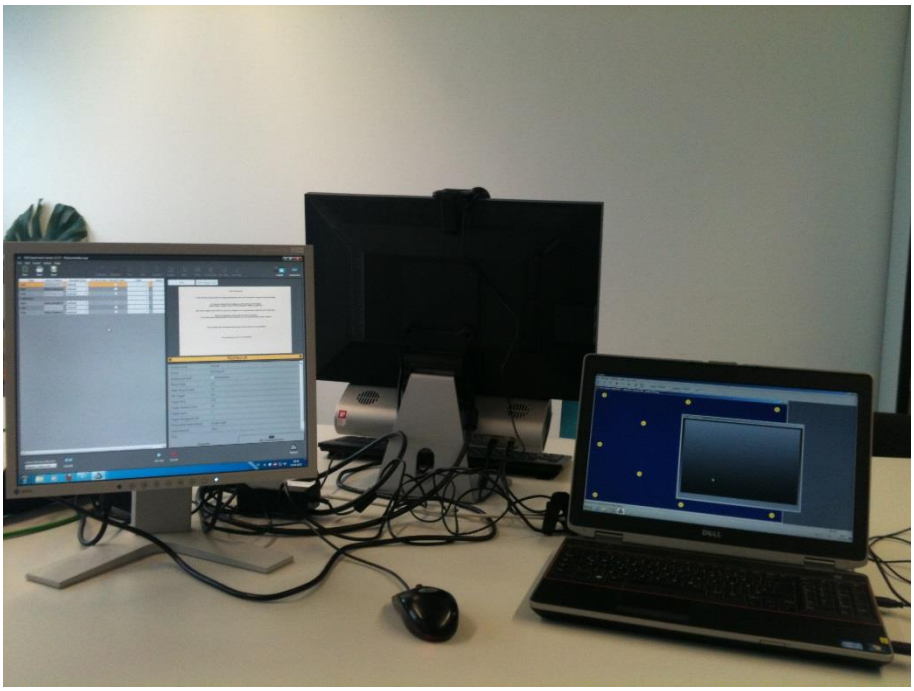


Abbildung 9. Versuchsaufbau aus Sicht der Versuchsleiterin (aus Magin, 2013).

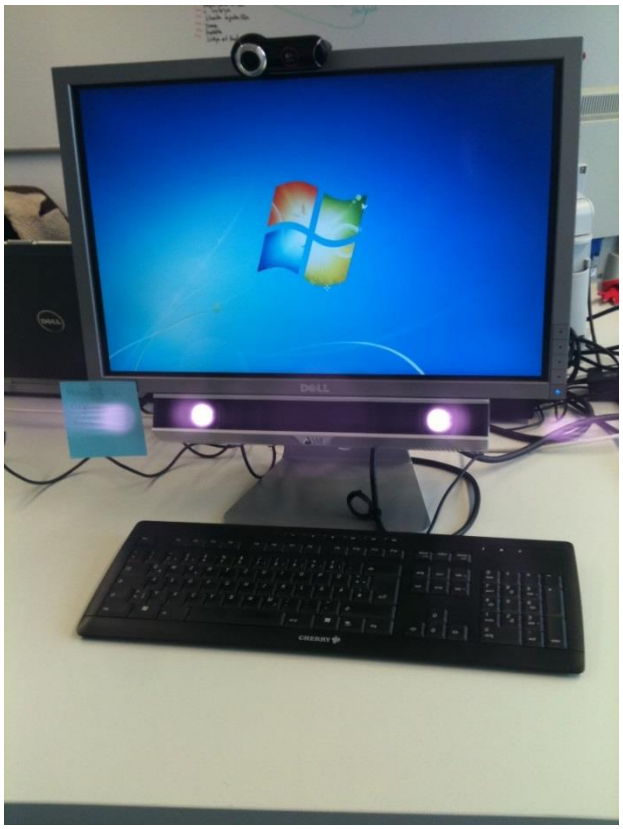


Abbildung 10. Versuchsaufbau aus Sicht der Teilnehmer (aus Magin, 2013).

4.2.1.2 Versuchsablauf

Zu Beginn eines Termins wurde der jeweilige Proband, bzw. die Probandin vor dem Haus oder am Fahrstuhl abgeholt und zum Untersuchungsraum begleitet. Dort konnten die Probanden erst einmal ankommen und sich einrichten, bevor ihnen der grobe Ablauf des bevorstehenden Termins umrissen wurde. Bevor der Versuch begann, unterschrieben die Teilnehmer zunächst eine Einverständniserklärung zur Erfassung und Verwendung ihrer Daten in Rahmen dieser Studie. Der Vordruck für die Einverständniserklärung ist im Anhang dieser Arbeit zu finden (siehe Anhang C). Die Erhebung begann danach am Bildschirm mit der Beantwortung der Fragen bezüglich der demografischen Attribute und dem ersten Teil der Interneterfahrung. Danach wurden die Teilnehmer im Rahmen des Fragebogens aufgefordert der Versuchsleiterin zu signalisieren, dass sie den Fragebogen beendet haben. Zu diesem Zeitpunkt wurde dann die Kalibrierung des Blickbewegungssystems vorgenommen. Nach erfolgreicher Kalibrierung wurden den Teilnehmern dann zwei Aufgaben gestellt, welche die Erfassung des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping ermöglichen sollten. Im Anschluss an die Aufgabenbearbeitung fand ein kurzes Interview statt. Hierin wurden die Probanden unter anderem gefragt, ob sie sich anders verhalten hätten, als sie dies zuhause tun würden. Der Rest des Interviews hatte einen Fokus, der im Rahmen dieser Arbeit keine Rolle spielt.
Den Abschluss des Versuchs bildeten dann die beiden anderen Fragebögen zur Erfassung des objektiven und subjektiven Wissens bezüglich des Datenschutzes und zur Einschätzung von Risiko, Nutzen und Wahrscheinlichkeit für die drei risikoreichen Handlungen. Der Fragebogen wurde in zwei Teilen dargeboten, um zu verhindern, dass die Probanden sich durch vorangegangene Fragen zu Datenschutz während der Bearbeitung der Aufgabe vorsichtiger verhalten, als sie das normalerweise tun würden.

Sowohl die Fragebögen als auch die Aufgabenbeschreibung und -bearbeitung fanden an demselben Bildschirmarbeitsplatz statt. Auf die häufig verwendete „Methode des lauten Denkens“ wurde verzichtet, da diese die Probanden in ihrer Aufgabenbearbeitung stören kann (Oehme & Jürgensohn, 2006). Stattdessen wurde während des gesamten Termins mittels der Webcam, die am Monitor vor ihrem Gesicht installiert war, gefilmt. Diese Aufnahmen beinhalten neben Bild auch Ton.
Die Termine dauerten je Proband ca. 1,5 Stunden. Nach Beendigung der gesamten Prozedur wurde sich bei den Probanden bedankt, sie wurden bezüglich dem Fokus der Studie aufgeklärt und konnten Fragen stellen. Im Anschluss wurde ihnen die Aufwandsentschädigung ausgehändigt und sie verabschiedet. Tabelle 11 stellt den gesamten Versuchsablauf noch einmal schematisch dar.

Tabelle 11. Versuchsablauf.

Phase der Erhebung	**Inhalte**	
Begrüßung und Beginn	Empfang	
	Beschreibung des Ablaufs	
	Einverständniserklärung	
Fragebogen 1. Teil	Demographische Attribute	Alter
		Geschlecht
		Einkommen
		Bildung
	Interneterfahrung	Nutzungsdauer
		Nutzungshäufigkeit
		Besitz internetfähiger Geräte
Kalibrierung des Blickbewegungssystems		
Aufgabenbearbeitung	1. Aufgabe	Suchen nach einem Produkt im Wert von 10€ auf einer bekannten Internetseite
	2. Aufgabe	Bestellen dieses Produkts auf einer unbekannten Internetseite
Interview		Haben Sie sich anders verhalten, als Sie das zuhause tun?
		Woran haben Sie sich beim Aussuchen der Webseite orientiert?
Fragebogen 2. Teil	Interneterfahrung	Wahrgenommenes Wissen
		Tatsächliches Wissen
	Einschätzung von risikoreichen Handlungen	Wahrgenommenes Risiko
		Erwarteter Nutzen
		Wahrscheinlichkeit für risikoreiche Handlung
Abschluss	Bedanken	
	Aufklärung und Fragen	
	Aufwandsentschädigung	
	Verabschiedung	

Um sowohl das gesamte Vorgehen zu überprüfen und der Versuchsleiterin die notwendige Sicherheit zu geben wurde der gesamte Versuch im Vorfeld der Erhebung dreimal im Rahmen eines Pre-Tests durchgeführt. Dieser führte nur zu marginalen Änderungen. Die erhobenen Daten flossen aber nicht in die tatsächliche Studie ein.

4.2.2 Verwendete Methoden

Es wurde eine Kombination aus Fragebogen, Interview und zweier online Aufgaben verwendet. Im Rahmen des Fragebogens wurden alle Bestandteile des Arbeitsmodells außer dem tatsächlichen Verhalten erfragt. Das tatsächliche Verhalten wurde mittels der Aufzeichnung der Blickbewegungen während der online Aufgaben in Kombination mit einem kurzen Interview erfasst.
Die Videoaufzeichnung diente als Sicherheit zur Klärung eventueller Störungen und als eventuelle Rückfallebene bei technischen Problemen.

4.2.2.1 Fragebögen

Mit Hilfe eines Fragebogens wurde sowohl nach dem Geburtsjahr, Geschlecht, Einkommen und aktuell höchstem Bildungsabschluss als auch nach der Häufigkeit und Dauer der online Nutzung sowie dem Besitz internetfähiger Geräte gefragt.
Bei der Art der Abfrage und den vorgegebenen Antwortmöglichkeiten wurde sich stark an den Unterscheidungskriterien der „Milieustudie zu Vertrauen und Sicherheit im Internet“ des Deutschen Institutes für Vertrauen und Sicherheit im Internet (DIVSI) (2012) orientiert. Dieses nahm eine Einteilung der deutschen Internetnutzer mit Hilfe von soziodemographischen Kriterien vor. Als Basis dienten die sogenannten Sinus-Milieus®, bei denen es sich um eine Kategorisierung der Einwohner eines Landes handelt, die im Kontext der Marktforschung entwickelt wurde. Als Ergebnis der repräsentativen Studie des DIVSI ergaben sich sieben Internet-Milieus zu Vertrauen und Sicherheit im Internet.
Ein weiterer Fragebogen diente der Erfassung des objektiven und subjektiven Wissens bezüglich des Datenschutzes. Dieser Fragebogen wurde in Zusammenarbeit von Psychologen und Informatikern entwickelt. Das war notwendig, da im Rahmen einer Literaturrecherche kein bereits verwendeter Fragebogen in diesem Kontext gefunden wurde. Es existieren bereits unterschiedliche Fragebögen zu *Internet/Web skills* (Novak, Hoffman & Yung, 2000; van Deursen & van Dijk, 2010), *Internet/Web knowledge* (Page, Robson & Uncles, 2012; Potosky, 2007) oder *consumer knowledge* (Page & Uncles, 2004; Pillai & Hofacker, 2007). Bei keinem von diesen wurde aber der Fokus auf Datenschutz gelegt. Zur Erstellung eines eigenen Fragebogens wurden deshalb zunächst Fakten über Gefahren in Bezug auf Datenschutz im Internet gesammelt. Als Quellen dienten hierfür unter anderem Berichte des Bundeskriminalamtes über Kriminalität im Internet und Warnhinweise von Bankwebseiten bzw. Browsern. Die gefundenen Gefahren wurden in einem nächsten Schritt in geeignete Items übersetzt. Bei der Auswahl dienten die in Page & Uncles (2004) genannten Kategorien (siehe Kapitel 2.1.7) als Orientierung. Diese ergeben sich, indem deklaratives und prozedurales Wissen (siehe Kapitel 2.1.7) zusätzlich jeweils in allgemeines und spezielles Wissen eingeteilt wird. In mehreren studentischen Arbeiten wurde der Fragebogen dann auf seine Güte getestet (Bäuerlein, Braun & Ziemek, 2013; Debel, Feldbusch, Ghafarian & Moghaddamkia, 2013; Goldstein, Wagenknecht, Schirmer & Wiecha, 2013) und entsprechend angepasst. Der im Rahmen dieser Studie auszuwertende Fragebogen enthält insgesamt 4 Items zum subjektiven (wahrgenommenen) und 10 Items zum objektiven (tatsächlichen) Wissen. Im Rahmen des subjektiven Wissens wurde der wahrgenommene individuelle Kenntnisstand bezüglich Verschlüsselung ('Ich weiß viel über Verschlüsselung im Internet.'), Angriffen im Internet, Man-in-the-

middle-Angriffen und dem Schutz der Privatsphäre auf einer visuellen Analogskala eingeschätzt. Die Skala war mit Werten von 1-50 hinterlegt. Die Anker der Skala lauteten jeweils „Stimme gar nicht zu“ (links der Skala) und „Stimme vollkommen zu“ (rechts der Skala). Eines der Items wurde dabei invertiert dargeboten („Ich verfüge über wenig Wissen über Man-in-the-middle-Angriffe“). Das bedeutet, dass im Gegensatz zu den anderen Items hier ein ausgeprägtes Wissen zur Nutzung der negativen („Stimme gar nicht zu“) Antworttendenz führen müsste. Dieses Mittels bedient man sich bei der Fragebogenkonstruktion, um den Verzerrungseffekt der Akquieszenz erkennen zu können (Moosbrugger & Kelava, 2007). Dieser wird auch Zustimmungseffekt genannt und äußert sich in der unkritischen Zustimmung der Items (Moosbrugger & Kelava, 2007).

Da in der Literatur kritisiert wird, dass Wissen häufig nur durch Selbsteinschätzung erhoben wird (z. B. Hargittai, 2005; van Deursen & van Dijk, 2010), wurde in dieser Studie Wert auf einen zusätzlichen Fragebogenteil gelegt, der das tatsächliche Wissen der Teilnehmer erfassen sollte. Die gestellten Fragen erfassten dabei sowohl deklaratives Wissen, wie z. B. Definitionen von Begriffen, als auch prozedurales Wissen, wie z. B. „Bei Unsicherheit, ob es sich um eine verschlüsselte Verbindung handelt, überprüfe ich,…“. Zur Beantwortung dieser Fragen wurden drei unterschiedliche Skalen verwendet. Bei drei Items waren die Antwortmöglichkeiten „stimmt“, „stimmt nicht“ und „weiß ich nicht“ vorgegeben. Bei drei weiteren wurde nach der richtigen Definition der Begriffe „Cookie“, „Spyware“ bzw. „Phishing“ gefragt. Die vorgegebenen möglichen Antworten waren bei allen drei Items gleich. Sie bestanden aus sieben kurzen Definitionen, wobei jeweils eine andere die Richtige war. Vervollständigt wurde die Auswahl durch die Antwortmöglichkeiten „Ich habe dieses Wort zuvor gesehen, weiß aber nicht, was es für Computer bedeutet.“, „Ich habe dieses Wort nie zuvor gesehen.“ und „Keine der genannten“. Die anderen vier Items wurden nach dem Multiple Choice Prinzip gestaltet. Hier waren vier oder fünf Antwortmöglichkeiten vorgegeben, von denen jeweils zwei Antworten richtig waren. Zu Beginn des Tests wurden die Probanden deshalb darauf hingewiesen, dass auch mehrere Antworten richtig sein können. Wie auch bei den beiden vorigen Fragetypen wurden die Antworten um die Möglichkeit „weiß ich nicht“ erweitert. Diese Antwortkategorie ist dann empfohlen, wenn davon ausgegangen wird, dass einige Probanden nicht in der Lage sind, die Frage richtig zu beantworten (Moosbrugger & Kelava, 2007). Es soll damit verhindert werden, dass diese gezwungen wären zu raten.

Neben den Wissensfragen wurde im Rahmen des Fragebogens auch um die Einschätzungen von drei unterschiedlichen risikoreichen Handlungen gebeten, die im Rahmen Datenschutz beim Onlineshopping existieren. Bei der Zusammenstellung derer wurde sich an den Hinweisen zum sicheren online Shoppen vom BSI orientiert (Bundesamt für Sicherheit in der Informationstechnik, o.D.b), die in Kapitel 2.3.3 bereits dargestellt wurden. Die Handlungen „Etwas online zu kaufen, ohne vorher die AGB zu lesen“, „im Internet Daten anzugeben, ohne vorher die Datenschutzerklärungen angeschaut zu haben“ und „vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt“ wurden in Bezug auf das *wahrgenommene Risiko*, den *erwarteten Nutzen* sowie bezüglich der *Wahrscheinlichkeit* dafür einschätzt, dieses Verhalten[2] selbst zu zeigen. Die Art der Abfrage orientierte sich dabei an der sogenannten Domains-Specific Risk-Taking Scale (DOSPERT; siehe Kapitel 2.4.1). Anders als in der originalen Fassung wurde im Rahmen dieser Studie jeweils eine visuelle Analogskala verwendet, bei der Werte zwischen 1-50 hinterlegt wurden. Die Anker lauteten hier „überhaupt kein Risiko“/„sehr hohes Risiko“, „gar keinen Nutzen“/„großen Nutzen“ und „sehr unwahrscheinlich“/„sehr wahrscheinlich“. Der Hauptgrund für die Verwendung dieser Skala war der, dass genau diese Skala schon im Rahmen anderer Teile des Fragebogens verwendet wurde und die

[2] angepasst an die im Rahmen der DOSPERT verwendeten Begrifflichkeit, wird in Bezug auf diese Variable *Verhalten*, statt richtigerweise *Handlung* verwendet.

Anzahl der verwendeten Antwortformate möglichst gering gehalten werden sollte. Darüber hinaus wurde sich von deren Verwendung versprochen, dass es den Probanden leichter fällt sich auf einer solchen Skala zu orientieren, als sich absolut einem Kästchen zuzuordnen. Zudem wurde erwartet, dass sich die Antworten mehr unterscheiden als bei der im Originalen verwendeten fünfstufigen Likertskala. Insgesamt wurden bei der Konstruktion der Fragebögen die von Moosbrugger und Kelava (2007, S. 56) zusammengefassten Zielvorgaben beachtet. Diese sind: „leichte Verständlichkeit, einfache Durchführbarkeit, kurze Lösungszeit, geringer Material-, bzw. Papierverbrauch, leichte Auswertbarkeit und die geringe Häufigkeit von Zufallslösungen".
Wie schon bei der Gewichtungsstudie wurde der gesamte Fragebogen mit Hilfe des Software-Pakets SoSci Survey (o.D.) konzipiert. Der gesamte Fragebogen ist in Anhang B dieser Arbeit zu finden.

4.2.2.2 Aufgabe

Die Aufgabe, die den Probanden im Rahmen der Studie gestellt wurde, hatte zum Ziel, der Erfassung des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping einen Rahmen zu geben, der die Teilnehmer außerdem von der Erfassung ihrer Blickbewegungen ablenkte. Zusätzlich sollten die in Kapitel 3.3 erarbeiteten Anforderungen an die Aufgabe erfüllt werden. Im ersten Schritt wurden die Teilnehmer deshalb gebeten, sich frei im Internet ein Produkt auszusuchen, welches sie für einen Betrag von 10€ selbst erwerben wollten („Ihre erste Aufgabe besteht darin, im Internet auf einer Verkaufsplattform ein Produkt im Wert von 10€ auszuwählen, das Sie auch wirklich erwerben möchten und welches für Sie einen persönlichen Nutzen generiert. Wenden Sie sich bitte an die Versuchsleiterin, sobald Sie damit fertig sind!). Der Betrag entsprach der Aufwandsentschädigung, die jeder Teilnehmer im Anschluss an den Versuch erhielt und die bereits im Vorfeld in Aussicht gestellt wurde. Hatte sich der jeweilige Proband irgendwann (es gab keine zeitliche Einschränkung), auf ein Produkt festgelegt, so wurde ihm, bzw. ihr die nächste Aufgabe ausgehändigt („Ihre zweite Aufgabe ist, das von Ihnen gewählte Produkt auf einer Internetseite, auf der Sie noch nichts bestellt haben, zu einem möglichst günstigen Preis zu bestellen. Hinweis: Die 10€ Aufwandsentschädigung erhalten Sie auf jeden Fall, auch wenn das bestellte Produkt weniger als 10€ kostet."). Mit der Einschränkung, der Webshops auf einen, bei dem bislang noch nicht bestellt wurde, sollte gewährleistet werden, dass es sich bei allen Teilnehmern um potentielle Kunden handelt. Laut Kim (2012) sind potentielle Kunden im Gegensatz zu Wiederholungskäufern jene, die bei diesem speziellen Anbieter noch nicht gekauft haben. Es besteht demnach nicht bereits ein Vertrauensverhältnis, so dass vor Angabe der personenbezogenen Daten eine Überprüfung des Shops stattfinden sollte. Wie von Holmqvist et al. (2011) empfohlen, wurden beide Aufgaben den Probanden schriftlich auf einem Blatt Papier von der Versuchsleiterin dargeboten. Diese Standardisierung sollte Verzerrungen in Bezug auf die Aufgabenstellung und möglichen Versuchsleitereffekten vorbeugen (Huber, 2005).

4.2.2.3 Blickbewegungsmessung

Die Blickbewegungsmessung wurde kurz vor der Stellung der ersten Aufgabe kalibriert, gestartet und am Ende der zweiten Aufgabe gestoppt. Zu Beginn der Kalibrierung wurden die Probanden gebeten, sich mit einem Abstand von ca. 70 cm gerade vor dem Bildschirm zu positionieren. Es wurde darauf hingewiesen trotzdem auf eine möglichst bequeme Haltung zu achten, da diese möglichst während der gesamten Aufgabenbearbeitung eingehalten werden soll. Auf dem Bildschirm der Versuchsleiterin waren im Kalibrierungsmodus zur Hilfestellung die Augen des Probanden mit Richtungspfeilen zur richtigen Positionierung angezeigt. Nachdem eine passende Sitzposition gefunden war, wurde eine 5-Punkt-

Kalibrierung durchgeführt. Dabei werden nacheinander fünf Punkte, in den vier Ecken und in der Mitte des Bildschirms dargeboten, auf die der jeweilige Proband blicken soll. Sobald ein Punkt fixiert wurde schreitet die Kalibrierung automatisch voran. Um möglichst exakte Ergebnisse zu erhalten wurde, bei der Blickbewegung so lange kalibriert, bis die Abweichung der aufgezeichneten Blicke zum dargestellten Stimulus weniger als 0,5° betrugen. Dieses Vorgehen entspricht dem von Velichkovsky et al. (2000), Tatler (2007) und Foulsham & Underwood (2008). Im Falle, dass die Probanden während der Bearbeitung der Aufgabe zu weit von der, bei der Kalibrierung eingenommenen Position abwichen, wurden sie von der Versuchsleiterin darauf hingewiesen. In den meisten Fällen war dies allerdings nicht notwendig und die Erfassung der Blickbewegungen fand ohne weitere Beeinflussung der Probanden statt.

4.3 Ergebnisse Explorationsstudie

Die im Rahmen der Explorationsstudie erfassten Daten wurden im Anschluss aufbereitet und mit Hilfe des Statistikprogrammes IBM SPSS Statistics ausgewertet. Die Ergebnisse sind in Tabelle 12 zusammengefasst und folgend in den Kapiteln 4.3.1-4.3.6 und 4.4 inhaltlich dargestellt.

Tabelle 12. Gesamte deskriptive Ergebnisse der Explorationsstudie.

n		50
Alter		19-65 (MW = 29,36; SD = 12,88)
Geschlecht	männlich	24 (48%)
	weiblich	26 (52%)
Bildung	"Noch Schüler"	
	"Schule beendet ohne Abschluss"	
	"Volks-, Hauptschulabschluss"	
	"Mittlere Reife, Realschul- oder gleichwertiger Abschluss"	
	"Abgeschlossene Lehre"	
	"Fachabitur, Fachhochschulreife"	8 (16%)
	"Abitur, Hochschulreife"	30 (60%)
	"Fachhochschul-/Hochschulabschluss"	12 (24%)
Einkommen	"nicht beantwortet"	
	"unter 1500€"	33 (66%)
	"1500€ bis unter 2000€"	3 (6%)
	"2000€ bis unter 2500€"	3 (6%)
	"2500€ bis unter 3000€"	5 (10%)
	"3000€ bis unter 3500€"	
	"3500€ bis unter 4000€"	1 (2%)
	"4000€ bis unter 4500€"	1 (2%)
	"4500€ bis unter 5000€"	
	"5000€ und mehr"	2 (4%)

Nutzungshäufigkeit	"täglich"	48 (96%)
	"mehrmals pro Woche"	2 (4%)
	"ein paar Mal pro Monat"	
	"seltener"	
Nutzungsdauer	"weniger als 3 Jahre"	
	"3 bis unter 7 Jahren"	11 (22%)
	"7 bis unter 10 Jahren"	16 (32%)
	"mehr als 10 Jahren"	23 (46%)
Besitz	Desktop-PC	20 (40%)
	Laptop/Notebook	48 (96%)
	Tablet-PC	7 (14%)
	Smartphone/Internetfähiges Telefon (z. B. iPhone, BlackBerry,…)	36 (72%)
	Spielekonsole (z. B. XBOX, Playstation, Game Cube,…)	10 (20%)
	"keines von diesen"	
Besitz gesamt		1-5 (MW=2,42; SD=1,03)
Wahrgenommenes Wissen		3-38 (MW = 17,50; SD = 9,53)
Tatsächliches Wissen		1,17-9,17 (MW = 5,62; SD = 2,12)
Wahrgenommenes Risiko	AGB_Etwas online kaufen, ohne vorher die AGB zu lesen	10-50 (MW = 30,94; SD = 11,20)
	DSErkl_Daten anzugeben, ohne Datenschutzerklärungen angeschaut zu haben	10-50 (MW = 34,50; SD = 10,80)
	vVerb_Vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt	24-50 (MW = 39,36; SD = 8,15)
Erwarteter Nutzen	AGB_Etwas online kaufen, ohne vorher die AGB zu lesen	1-39 (MW = 15,21; SD = 11,73)
	DSErkl_Daten anzugeben, ohne Datenschutzerklärungen angeschaut zu haben	1-50 (MW = 15,73; SD = 11,98)
	vVerb_Vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt	1-50 (MW = 11,72; SD = 11,19)

Wahrscheinlichkeit	AGB_Etwas online kaufen, ohne vorher die AGB zu lesen	1-50 (MW =36,64 SD = 16,07)
	DSErkl_Daten anzugeben, ohne Datenschutzerklärungen angeschaut zu haben	1-50 (MW =29,64 SD = 14,89)
	vVerb_Vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt	1-50 (MW =21,12; SD = 15,11)

4.3.1 Ergebnisse bezüglich der demographischen Attribute

Für die Teilnahme an der Explorationsstudie konnten 50 Teilnehmer gewonnen werden. Mit 26 weiblichen Probandinnen (52%) und 24 männlichen (48%) ist das Geschlechterverhältnis dabei nahezu ausgeglichen. Das Alter der Probanden reicht von 19 Jahren bis zu 65 Jahren bei einem Mittelwert von 29,36 Jahren und einer Standardabweichung von 12,88 Jahren. Der Median beträgt 24 Jahre. Ein Shapiro-Wilk-Test auf Normalverteilung wurde mit $p<.000$ signifikant. Das bedeutet, dass die Altersverteilung nicht der Normalverteilung entspricht. In Bezug auf die Bildung erweisen sich die Probanden insgesamt als ausschließlich höher gebildet. So wird als höchster Bildungsabschluss von acht Personen (16%) das Fachabitur, bzw. die Fachhochschulreife angegeben. Abitur, bzw. die Fachhochschulreife besitzen 30 Personen (60%) und die restlichen 12 (24%) einen Fachhochschul- bzw. Hochschulabschluss. Wie zu erwarten war, konnte auch hier mittels des Shapiro-Wilk-Tests keine Normalverteilung nachgewiesen werden ($p<.000$). Beim Haushaltsnettoeinkommen gibt es Nennungen in allen Kategorien. Die meisten Probanden (66%) liegen hier bei unter 1500€. Auch diese Verteilung folgt nicht dem Verlauf einer Normalverteilung ($p<.000$)

4.3.2 Ergebnisse bezüglich der Erfahrung

Das Internet wird von den teilnehmenden Probanden regelmäßig genutzt. Bei zweien (4%) beschränkt sich die Nutzung dabei auf mehrmals pro Woche, während die restlichen 48 Personen (96%) täglich das Internet nutzen. In Bezug auf die Dauer der Internetnutzung gaben 11 Personen (22%) an, dies bereits seit drei bis hin zu sieben Jahren zu tun. Zwischen sieben und 10 Jahre lang nutzen 16 Teilnehmer (32%) und mehr als 10 Jahre 23 Probanden (46%) das Internet.
Um sich ein Bild darüber machen zu können, mit welchen und mit wie vielen Geräten die Probanden das Internet nutzen, wurde der Besitz internetfähiger Geräte abgefragt. Einen Desktop-PC besitzen 20 Personen (40%), einen Laptop, bzw. Notebook 48 Personen (96%), einen Tablet-PC 7 Personen (14%), ein Smartphone, bzw. ein internetfähiges Telefon besitzen 36 (72%) und eine Spielekonsole 10 Personen (20%). Kein Proband gab an, keines dieser Geräte zu benutzen. Für die weitere Berechnung wird aus den jeweiligen Angaben zu den einzelnen Geräten für jeden Probanden ein Gesamtwert über die Anzahl internetfähiger Geräte in seinem Besitz gebildet. Daraus ergibt sich die Verteilung, die unter Abbildung 11 dargestellt ist (Shapiro-Wilk-Test $p=.003$).

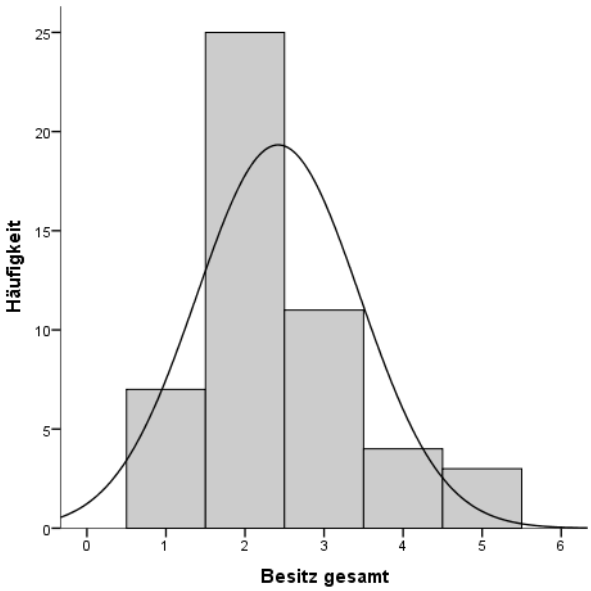


Abbildung 11. Verteilung der errechneten Gesamtanzahl internetfähiger Geräte.

Bezüglich des durchgeführten Wissenstests werden für jeden Teilnehmer zwei Werte ermittelt. Einer davon macht jeweils eine Aussage über das subjektive oder wahrgenommene Wissen der jeweiligen Person. Um diesen Wert bezüglich des subjektiven Wissens ermitteln zu können, werden die vier Einschätzungen, die die Probanden vorgenommen haben zu einer Skala zusammengefasst. Da es sich bei „Item 3“ um ein invertiertes Item handelt, wurde es vorher entsprechend umcodiert. Mittels einer Reliabilitätsanalyse wird dann die interne Konsistenz dieser Skala ermittelt. Dabei werden die Zusammenhangsstrukturen der Items untersucht. Jedes Item wird dafür als eigener Testteil gesehen. Der Wert für die interne Konsistenz, das sogenannte Cronbach`s Alpha steigt, je höher die einzelnen Items durchschnittlich miteinander korrelieren (Moosbrugger & Kelava, 2007). Die Skala mit den vier Items zum subjektiven Wissen erreicht nur ein Cronbach`s Alpha von .633. Schließt man „Item 3“ aber von der Skala aus, wird ein Cronbach`s Alpha von .819 erreicht. Der Ausschluss dieses Items hat darüber hinaus den Vorteil, dass damit einige fehlende Werte in der Berechnung entfallen. Scheinbar war es einigen Probanden schwergefallen, das invertierte Item auf der Skala zu bewerten. Da es sich demnach nur um drei Items handelt und eine punktgenaue Unterscheidung von Probanden mittels dieses Faktors nicht notwendig ist, wird in Anlehnung an Cortina (1993) eine ausreichend hohe interne Konsistenz angenommen.

Der Wert, der das subjektive Wissen des jeweiligen Probanden symbolisiert, entspricht also dem Mittelwert der individuellen Antworten auf die drei Items der Skala. Die sich ergebenden Werte reichen (auf der Skala von 0 bis 50) von 3 bis zu 50. Der Mittelwert der erhaltenen Verteilung beträgt 20,46 bei einer Standardabweichung von 11,18. Der Median liegt bei 17,83. Ein Shapiro-Wilk-Test kam mit einem $p=.406$ nicht zu einem signifikanten Ergebnis. Das bedeutet, dass die Werte einer Normalverteilung folgen.

Der zweite Wissenskennwert, der für jeden Probanden ermittelt wird, steht für das objektive oder tatsächliche Wissen. Dieser errechnet sich aus der Beantwortung der 10 Wissensfragen (siehe Kapitel 4.2.2.1). Hierbei werden die unterschiedlichen Fragetypen unterschiedlich bewertet. Bei den drei Fragen, bei denen die Antwortmöglichkeiten „stimmt“, „stimmt nicht“ und „weiß ich nicht“ vorgegeben waren, erhalten die Probanden für die richtige Antwort einen Punkt. Eine falsche Antwort oder das Ankreuzen der „weiß ich nicht“-Option ergibt keine Punkte. Entsprechend gibt es bei den drei Fragen

nach der jeweils richtigen Definition nur für die richtige Antwort einen Punkt. Alle anderen Optionen ergeben keine Punkte. Bei den Items im Multiple Choice Format waren immer zwei Antworten richtig. Für das Ankreuzen jeder dieser richtigen Antworten bekommen die Probanden je 0,5 Punkte, so dass die völlig richtige Beantwortung der Frage zu einem Punkt führt. Im Fall der Multiple Choice Fragen bekommen die Probanden auch Negativ-Punkte bei falscher Beantwortung. Abhängig davon, ob die Frage drei oder nur zwei falsche Antworten enthielt, wurden pro angekreuzter falscher Antwort -0,33, bzw. -0,5 Punkte vergeben. Als Gesamtscore bezüglich des tatsächlichen Wissens wurde im weiteren Verlauf für jeden Probanden die sich aus der Beantwortung der Fragen ergebende Gesamtsumme verwendet. Da es vier Multiple Choice Fragen gab, die zu je einem negativen Punkt führen könnten, liegt das Minimum der erreichbaren Punkte bei -4. Im Fall, das alle Fragen richtig beantwortet werden, ergibt sich das Maximum von 10 Punkten. Bei den im Rahmen der Studie erhaltenen tatsächlichen Werten liegt das Minimum bei 1,17 und das Maximum bei 9,17 Punkten. Der Mittelwert beträgt 5,62 bei einer Standardabweichung von 2,12 Punkten. Der Median liegt bei 5,92 Punkten. Ein Shapiro-Wilk-Test zeigte mit $p=.726$ kein signifikantes Ergebnis. Demnach kann davon ausgegangen werden, dass die Verteilung der Werte einer Normalverteilung gleicht.

4.3.3 Ergebnisse bezüglich der Einschätzungen der Risikosituationen

Neben den Fragen zu wahrgenommenem und tatsächlichem Wissen schätzten die Teilnehmer der Studie auch drei risikoreiche Handlungen beim Onlineshopping bezüglich des wahrgenommenen Risiko, des erwarteten Nutzens und der Wahrscheinlichkeit dieses Verhalten zu zeigen ein. Es zeigt sich, dass das wahrgenommene Risikos jeweils recht ähnlich hoch eingestuft wurde (MW AGB=30,94; MW DSErkl=34,50 und MW vVerb=39,36 auf Skala 0=„überhaupt kein Risiko“ bis 50=„sehr hohes Risiko“). Auch die im Vergleich zum Risiko geringeren Mittelwerte bezüglich des erwarteten Nutzens unterscheiden sich augenscheinlich kaum (MW AGB=15,21; MW DSErkl=15,73 und MW vVerb=11,72 auf Skala 0=„gar keinen Nutzen“ bis 50=„großen Nutzen“). Abweichungen zeigen sich bei den Wahrscheinlichkeiten dafür, das jeweilige Verhalten zu zeigen (MW AGB=36,64; MW DSErkl=29,64 und MW vVerb=21,12 auf Skala 0=„sehr unwahrscheinlich“ bis 50=„sehr wahrscheinlich“). Der durchgeführte Shapiro-Wilk Test bezüglich Normalverteilung ergab, dass alle Variablen außer der *Wahrscheinlichkeit etwas online zu kaufen, ohne vorher die AGB zu lesen* (p=.000) und dem *erwarteten Nutzen vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt* (p=.011) normalverteilt sind.

4.3.4 Ergebnisse bezüglich der Aufgabe

Grundlage für die bis hierhin vorgestellten deskriptiven Ergebnisse sind die Daten aller 50 Probanden, die erhoben wurden. Voraussetzung für die Nutzung der dazugehörenden Blickbewegungsdaten war, dass die gestellten Aufgaben bezüglich der Auswahl und dem Kauf eines Produktes für 10€ zufriedenstellend bearbeitet wurden. Da das gezeigte Verhalten tatsächliches Verhalten darstellen soll, wurden die Teilnehmer im Anschluss an die Aufgabenbearbeitung gefragt, ob sie sich anders verhalten hätten, als sie dies im entsprechenden Kontext zuhause tun. Die Daten der Probanden, die diese Frage bejahten, wurden aus der Analyse der Blickbewegungen ausgeschlossen. Zusätzlich gab es Probanden, bei denen sich im Anschluss zeigte, dass sie während der Suche nach einem seriösen Anbieter nicht wirklich davon ausgegangen waren, dass sie das Produkt tatsächlich kaufen sollten. Da auch in diesem

Fall nicht davon ausgegangen werden kann, dass tatsächliches Verhalten abgebildet werden konnte, wurden auch die Daten dieser Teilnehmer von der weiteren Analyse ausgeschlossen. Dasselbe galt auch für Probanden, die in dem Moment, in dem sie Daten angeben sollten, den Versuch von sich aus abbrachen. Auch hier kann in Bezug auf die Auswahl des Webshops nicht zweifelsfrei von tatsächlichem Verhalten ausgegangen werden. In einem weiteren Fall zeigte sich erst während des Interviews, dass der Proband normalerweise nie online Produkte erwirbt, was ebenfalls zum Ausschluss seiner Daten führte. Bedauerlicherweise lagen bei fünf weiteren Teilnehmern technische Probleme vor, welche die Auswertung der Daten verhinderten. Zur anschließenden Analyse der Blickbewegungen konnten deshalb nur die Daten von 32 Probanden verwendet werden. Da diese als Basis für die folgenden Analysen dienen, sind ausschließlich deren deskriptive Daten noch einmal in Tabelle 13 zusammengefasst.

Tabelle 13. Deskriptive Ergebnisse der Explorationsstudie bezogen auf die für die Blickbewegungsanalyse herangezogenen Teilnehmer.

n		32
Alter		19-62 (MW = 25,79; SD = 8,43)
Geschlecht	männlich	14 (43,8%)
	weiblich	18 (56,3%)
Bildung	"Noch Schüler"	
	"Schule beendet ohne Abschluss"	
	"Volks-, Hauptschulabschluss"	
	"Mittlere Reife, Realschul- oder gleichwertiger Abschluss"	
	"Abgeschlossene Lehre"	
	"Fachabitur, Fachhochschulreife"	5 (15,6%)
	"Abitur, Hochschulreife"	22 (68,8%)
	"Fachhochschul-/Hochschulabschluss"	5 (15,6%)
Einkommen	"nicht beantwortet"	
	"unter 1500€"	25 (78,1%)
	"1500€ bis unter 2000€"	1 (3,1%)
	"2000€ bis unter 2500€"	1 (3,1%)
	"2500€ bis unter 3000€"	3 (9,4%)
	"3000€ bis unter 3500€"	
	"3500€ bis unter 4000€"	
	"4000€ bis unter 4500€"	1 (3,1%)
	"4500€ bis unter 5000€"	
	"5000€ und mehr"	
Nutzungshäufigkeit	"täglich"	31 (96,9%)
	"mehrmals pro Woche"	1 (3,1%)
	"ein paar Mal pro Monat"	
	"seltener"	

Nutzungsdauer	"weniger als 3 Jahre"	
	"3 bis unter 7 Jahren"	8 (25,0%)
	"7 bis unter 10 Jahren"	12 (37,5%)
	"mehr als 10 Jahren"	12 (37,5%)
Besitz	Desktop-PC	10 (31,3%)
	Laptop/Notebook	31 (96,6%)
	Tablet-PC	5 (15,6%)
	Smartphone/Internetfähiges Telefon (z. B. iPhone, BlackBerry,…)	24 (75,0%)
	Spielekonsole (z. B. XBOX, Playstation, Game Cube,…)	6 (18,8%)
	"keines von diesen"	
Besitz gesamt		1-5 (MW=2,38; SD=.907)
Wahrgenommenes Wissen		3-38 (MW=19,89; SD=10,63)
Tatsächliches Wissen		1,17-9,17 (MW=5,67; SD=2,15)
Tatsächliches Verhalten		0-4 (MW=1,47; SD=1,24)
Wahrgenommenes Risiko	Etwas online kaufen, ohne vorher die AGB zu lesen	10-50 (MW=30,34; SD=11,73)
	Daten anzugeben, ohne Datenschutzerklärungen angeschaut zu haben	10-50 (MW=32,66; SD=11,40)
	Vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt	25-50 (MW=39,53; SD=7,59)
Erwarteter Nutzen	Etwas online kaufen, ohne vorher die AGB zu lesen	1-38 (MW=17,17; SD=11,31)
	Daten anzugeben, ohne Datenschutzerklärungen angeschaut zu haben	1-36 (MW=15,27; SD=10,87)
	Vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt	1-36 (MW=10,52; SD=9,42)
Wahrscheinlichkeit	Etwas online kaufen, ohne vorher die AGB zu lesen	1-50 (MW=42,34; SD=11,34)
	Daten anzugeben, ohne Datenschutzerklärungen angeschaut zu haben	1-50 (MW=34,47; SD=13,07)
	Vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt	1-50 (MW=25,61; SD=13,80)

Es ergaben sich daraus nur geringe Änderungen. So verringerte sich der Anteil der Personen, die über einen Fachhochschul- oder Hochschulabschluss verfügen. Dies schlägt sich gleichzeitig in einer Verringerung der Personen nieder, die tendenziell mehr verdienen. Höchstwahrscheinlich auch damit zusammenhängend fallen in der Gruppe der Teilnehmer, die das Internet bereits seit mehr als 10 Jahren nutzen die meisten Teilnehmer weg, was aber zu einer verbesserten Ausgeglichenheit bezüglich dieser Variable führt. In Bezug auf den Nutzen *Daten anzugeben, ohne Datenschutzerklärungen angeschaut zu haben* und *vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt* wird die vorhandene Skala von 1-50 nun nicht mehr ganz ausgenutzt. Dies schlägt sich aber in den Werten des jeweiligen Mittelwertes, bzw. der Standardabweichung nur gering nieder.

4.3.5 Ergebnisse bezüglich der Blickbewegung

Um neben den unabhängigen Variablen des Modells auch die abhängige Variable des tatsächlichen Verhaltens mit Werten abbilden zu können, werden die aufgezeichneten Blickbewegungen der Probanden analysiert. Von Interesse ist es dabei, ob und wenn ja, wie intensiv die Probanden sich der Vertrauenswürdigkeit des jeweiligen Webshops, bei dem sie Ihre Daten angegeben hätten, versichert haben. Im Rahmen dieser Studie wird dabei die Messgröße der Fixation als Basis verwendet, da während dieser die Informationsaufnahme stattfindet (Helo et al., 2014). Einen weiteren Grund für die Verwendung von Fixationen stellt die verwendete Abtastrate von 120Hz dar. Laut Handbuch der Eye-Tracking Software BeGaze™ von SMI gehört dies zu „low speed event detection“, wofür ein auf Streuungswerte basierender Auswertungsalgorithmus empfohlen wird. Dieser sucht demnach zuerst nach vorhandenen Fixationen. Um den Aufwand der Auswertung etwas einzuschränken, werden dabei nur die Webshops analysiert, bei denen die Teilnehmer sich bereit zeigten, ihre Daten anzugeben.
Für jeden Probanden und jede Probandin wird dafür zunächst der entsprechende Webshop ermittelt, bei dem die Probanden ihre Daten angeben wollten, bevor der Versuch von der Versuchsleiterin abgebrochen wurde. Im nächsten Schritt wird jede besuchte Seite dieser Webshops bezüglich der AOIs bearbeitet. Die Auswertungssoftware BeGaze™ von SMI liefert dazu von jeder Seite einen Screenshot, der als Datei im .jpg-Format abgespeichert wurde. Darauf wird auf jeden vorhandenen Hinweis ein entsprechend großes AOI-Feld gelegt. Kommt ein Hinweis mehrfach auf einer Seite vor, gibt es auch mehrere entsprechend benannte AOI-Felder. Abbildung 12 zeigt einen der Screenshots mit den entsprechend gelegten AOI.
Beim Legen der jeweiligen AOI wird sich an den Hinweisen von Holmqvist et al. (2011) orientiert. Diese besagen, dass jede AOI eine Fläche mit homogener Bedeutung abdecken soll, die AOI so präzise wie möglich gelegt werden sollen und diese nicht zu nahe beieinander liegen bzw. sich nur, wenn es unbedingt notwendig ist, überlappen sollen. Außerdem soll eine AOI nicht über verschiedene Areale des Stimulus verteilt werden, wenn es keinen klaren Bedeutungszusammenhang gibt. In dem Fall, wo z. B. ein und dasselbe Gütesiegel mehrfach abgebildet ist, ist dieser allerdings gegeben.
Teilweise sind die verwendeten Hinweise recht breit formuliert. Im Rahmen der Legung der AOI-Felder werden demnach verschiedene Teile des Webshops als zur gleichen AOI gehörend benannt. So fließen in die AOI *Informationen zu Datenschutz und Datensicherheit* zum Beispiel unterschiedlich benannte Links zu diesen Informationen, verschiedene schriftliche, bzw. ausformulierte Hinweise auf Verschlüsselung (z. B. „Ihre Daten werden verschlüsselt (256 Bit SSL)“) oder Datenschutz (Hinweis: „Der persönliche Benutzername ist öffentlich sichtbar“) sowie tatsächlich ausformulierte Datenschutzhinweise ein.

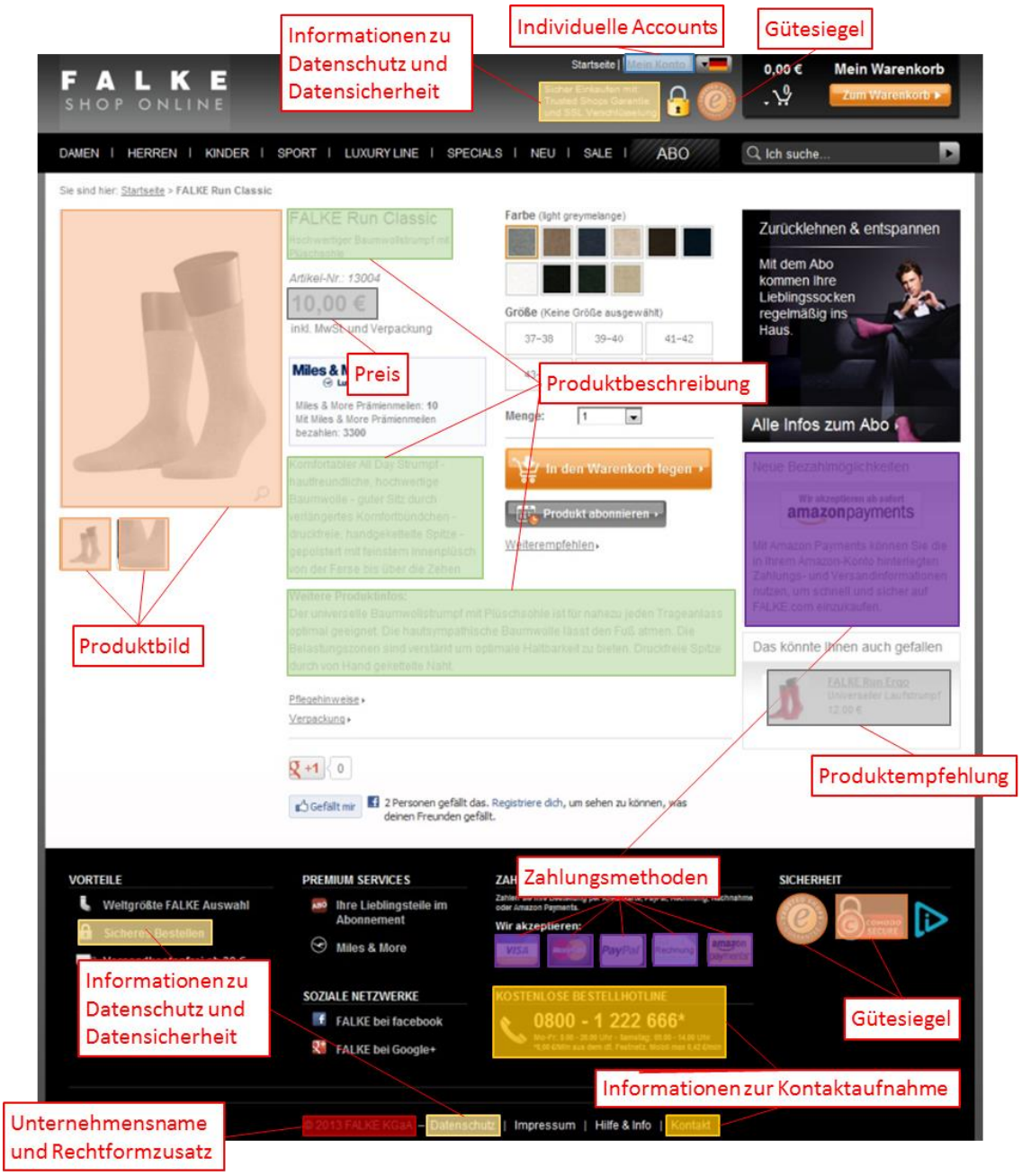


Abbildung 12. Screenshot einer Webseite mit den entsprechenden Areas of Interests (AOI).

Die Software ist in der Lage, für jede der AOI entsprechende Blickbewegungsdaten auszugeben. Von den vielen angebotenen Messgrößen werden im Rahmen der Auswertung die Größen *Anzahl Fixationen (Fixation count)*, *Dauer Fixationen (Fixation time [ms])*, *Rang (Sequence)* und *Normalized Dwell Time [ms/Coverage]* verwendet. Für die Anzahl und Dauer der Fixationen werden alle im AOI liegenden Fixationen aufsummiert. Für den Rang wird die Reihenfolge betrachtet, in der die verschiedenen AOI fixiert wurden. Der Rang entspricht der jeweiligen Stelle des AOI in dieser Reihenfolge. Bei der *Normalized Dwell Time* handelt es sich um ein aus mehreren Größen zusammengesetztes Maß. Grundlage bildet die sogenannte *Dwell Time* (Verweilzeit; siehe auch Kapitel 2.5.3). Im Rahmen des verwendeten Algorithmus ist diese als die Summe aller Fixationen und Sakkaden innerhalb einer AOI definiert. Die AOI sind allerdings unterschiedlich groß. Allein aufgrund der Größe ist die Wahrscheinlichkeit, dass Fixationen innerhalb einer sehr großen AOI stattfinden, entsprechend höher,

als bei einer sehr kleinen AOI (Holmqvist et al., 2011). Birmingham, Bischof, and Kingstone (2009) gehen mit diesem Problem um, indem sie die AOI Größe normalisieren, indem sie die Anzahl Fixationen in der entsprechenden Region durch die Anzahl aller Fixationen teilen. Die Software BeGaze gibt hierfür die Messgröße *Coverage* [%] aus. Diese setzt die Größe der jeweiligen AOI mit der Gesamtgröße des jeweiligen Stimulus ins Verhältnis. Die Normalisierung der *Dwell Time* findet dann statt, indem sie nicht auf die absolute Größe der AOI sondern auf dieses Verhältnismaß angewendet wird. Für die Normalisierung in Bezug auf Position gibt es bislang keine Vorschläge (Holmqvist et al., 2011).
Da, im Normalfall davon auszugehen ist, dass beide Augen sich gleichzeitig bewegen, reicht es aus, nur die Bewegungen eines Auges aufzuzeichnen (Holmqvist et al., 2011). Ausnahmen hiervon stellen die Arbeiten mit Kindern dar, bei denen die Distanzen der Blickpositionen noch größer als bei Erwachsenen sind oder klinische Studien zu Fehlsichtigkeiten, bzw. Studien, die auf der Messung sehr kleiner Unterschiede basieren. Im Rahmen dieser Studie wurden zunächst die Positionen beider Augen aufgezeichnet und von der Software ausgegeben. Um eventuelle Fehler ausschließen zu können, werden dann für jeden Probanden die Daten des rechten und des linken Auges verglichen. Da sich bei niemandem nennenswerte Abweichungen zeigen, werden die Daten auf die des jeweiligen rechten Auges reduziert. Tabelle 14 stellt die, über alle verbleibenden 32 Probanden zusammengefassten, Blickbewegungsdaten bezüglich der analysierten Hinweise dar. Die ersten beiden Spalten geben dabei an, bei wie vielen der Probanden der jeweilige Hinweis auf einer der Seiten des Webshops vorhanden war, bzw. wie viele der Probanden diesen Hinweis mindestens einmal fixierten. Von den Messgrößen *Anzahl Fixationen*, *Dauer Fixationen*, *Rang* und *Normalized Dwell Time* wurden jeweils die Mittelwerte gebildet.
Es zeigt sich, dass nur fünf der Hinweise (*https*, *Preis*, *Produktbeschreibung*, *Produktbild* und *Shopname (URL)*) bei allen Webshops vorhanden waren. Die Hinweise *Besucherzähler*, *Bonusprogramm* und *Look-in-Feature* kamen nur jeweils einmal vor. Auf keiner der besuchten Webshop-Seiten konnten die Hinweise *Gewerberegister und –nr*. und *Umsatzsteueridentifikationsnummer* gefunden werden.
Während einige Hinweise immer vorhanden waren, gab es keinen Hinweis, der von allen Probanden fixiert wurde. Fast alle Probanden schauten auf die *Produktbeschreibung* (31), den *Preis* (30) und das *Produktbild* (29). Niemand fixierte dagegen die ohnehin nur einmal, bzw. zweimal vorhandenen Hinweise *Besucherzähler* und *RSS-Feed*. Die Angabe der Anzahl der Fixationen in der darauffolgenden Spalte bezieht sich nur auf die Probanden, die den jeweiligen Hinweis überhaupt fixiert haben. Hier zeigt sich, dass deren Blicke am häufigsten die Hinweise bezüglich der *Rückgaberechte* (durchschnittlich 7 Fixationen) anvisierten. Auch die Hinweise bezüglich *individuelle[r] Accounts* (durchschnittlich 5,55 Fixationen) und *Veröffentlichungen von Expertenbeurteilungen, unabhängigen Testberichten, Preisen und Awards* (durchschnittlich 4,5 Fixationen) zogen die Blicke häufiger auf sich. Die längste Dauer der Betrachtung ergab sich hier für Hinweise bezüglich der *Rückgaberechte*. Auch die Hinweise bezüglich *individueller Accounts* und die *Produktbeschreibungen* wurden verhältnismäßig lange Zeit fixiert. Hinweise bezüglich *Bonusprogrammen* und auch *Produktempfehlungen* wurden selten und auch nur kurz fixiert.

Die nächste Spalte offenbart eine Schwierigkeit, die sich im Rahmen der Auswertung ergab. Die Screenshots der Webseiten enthielten leider nur die Webinhalte, nicht aber die Browsermaske. Für die Hinweise *EV-SSL-Zertifikat*, *https* und *Shopname (URL)* konnten demnach keine AOI gelegt werden. Im Rahmen einer Videoanalyse des aufgezeichneten Blickverhaltens konnten aber eventuelle Fixationen auf diese Hinweise nachvollzogen werden. Das galt allerdings nur für die Anzahl der Fixationen, nicht aber für deren Dauer oder den Rang. Aus dem Grund sind die entsprechenden Spalten bezüglich dieser Hinweise ungefüllt.

Tabelle 14. Blickbewegungsdaten der Explorationsstudie bezüglich der Hinweise auf die Vertrauenswürdigkeit eines Webshops (Vpn = Anzahl der Versuchspersonen, Fix. = Fixationen, NDwell Time = Normalized Dwell Time).

AOI	Vorhanden	Vpn	Anzahl Fix.	Dauer Fix. [ms]	Rang	NDwell Time [ms/Coverage]	Revisits
AGB	27	4	1,88	367,06	4,75	477817,34	0,75
Bestellfortschrittsanzeige	14	7	2,63	543,21	3,00	40848,52	1,25
Besucherzähler	1						
Bonusprogramm	1	1	1,00	108,50	8,00	3596,50	0,00
EV-SSL-Zertifikat	10	1	1,00				0,00
Expertenbeurteilungen…	14	5	4,50	909,20	6,67	83781,90	0,83
FAQ bzw. Hilfe	26	2	3,50	579,65	10,00	132873,85	1,50
Firmeninformationen	21	3	2,17	551,97	7,83	364195,67	0,33
Garantien	10	2	1,50	433,85	4,00	225297,20	0,00
Gewerberegister & –nr.	0						
Gütesiegel	21	5	2,33	750,79	5,33	160185,88	0,33
https	32	4	1,00				0,00
Individuelle Accounts	28	11	5,55	1437,52	4,32	618773,65	1,77
Info Datenschutz	27	10	2,79	702,45	3,84	196180,90	1,05
Internetbezahlsysteme	18	6	4,50	1273,19	5,50	570762,25	2,13
Kontakt	29	6	1,88	420,17	8,00	432612,18	0,25
Kundenbeurteilungen	15	8	4,23	1229,60	6,63	466995,54	0,66
Links verwandter Websites	26	2	1,50	567,32	5,50	1617243,51	0,00
Look-in-Feature	1	1	2,00	609,10	10,00	36822,80	1,00
MwSt bzw. USt	16	8	1,19	348,40	4,33	635787,48	0,14
Name/Anschrift Anbieters	24	3	3,25	1042,45	8,75	973507,88	1,50
Preis	32	30	1,73	539,78	8,86	1362400,05	0,58
Produktbeschreibung	32	31	4,78	1436,03	9,32	392483,11	1,19
Produktbild	32	29	4,43	1351,64	10,42	254142,15	1,72
Produktempfehlungen	6	1	1,00	141,80	6,00	189829,40	0,00
RSS-Feed	2						
Rückgaberechte	14	1	7	1668,34	6	357187,45	6
Rücksendekosten	16	4	1,00	204,38	4,50	391176,01	0,00
Shopname (URL)	32	10	1,00				0,00
Social Bookmarks	9	1	2,50	517,25	18,25	866874,38	1,25
Sprachoptionen	6	2	1,00	325,37	3,67	439403,40	0,00
Suchfunktion	24	20	2,38	742,80	4,29	214262,63	0,76
Unternehmensname	27	16	1,88	477,47	4,52	156393,58	0,45
Ust.IdNr.	0						
Verfügbarkeitsanzeige	24	19	1,51	422,15	7,25	1031699,19	0,37
Versandkosten	29	23	2,30	727,73	5,77	774021,61	0,48
Versandoptionen	20	8	2,63	685,10	5,56	692988,51	1,00
Widerrufsrecht	17	2	1,50	358,80	8,50	302156,35	0,00
Zahlungsmethoden	26	12	2,92	952,24	5,73	500828,92	1,23
Zusatzkosten	7	1	2	508,9	6	293948	1

Schaut man sich die Rangreihen an, in denen die Hinweise fixiert wurden, so zeigt sich, dass die Hinweise *Bestellfortschrittsanzeige*, *Sprachoptionen* und *Informationen zu Datenschutz/Datensicherheit* eher früh fixiert wurden. *Social Bookmarks*, *Look-in-Features*, aber auch *Produktbilder* wurden dagegen eher später betrachtet. Rechnet man die unterschiedliche Größe der AOI aus den Blickdaten heraus, zeigt sich, dass den *Links zu verwandten Webseiten* die meiste Zeit gewidmet wurde. Auch lange beschäftigten sich die Probanden mit dem *Preis* und der *Verfügbarkeitsanzeige*. Dem Hinweis der *Bonusprogramme* wurde von allen betrachteten Hinweisen am wenigsten Zeit gewidmet. In Bezug auf die Häufigkeit, in der die Blicke sich wieder zurück in ein bereits betrachtetes AOI bewegten, lässt sich sagen, dass dies am häufigsten bei Hinweisen zu *Rückgaberechten* der Fall war. Hier muss allerdings erwähnt werden, dass die Angabe der Revisits dahingehend verzerrt ist, als dass hier nur Wiedereintritte in ein bereits besuchtes AOI gezählt werden. Gab es auf einer Seite dieselbe AOI mehrfach und mehrere davon wurden fixiert, so zählte dies nicht als Revisit.

4.3.6 Ergebnisse bezüglich des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping

Die Überprüfung der Anzahl fixierter wichtigster Hinweise führt zu dem Ergebnis, dass keiner der 32 Probanden, die bereit waren ein Produkt im Rahmen des Versuchs zu kaufen und dafür ihre Daten anzugeben, alle acht Hinweise im Vorfeld überprüfte. Die höchste Anzahl überprüfter wichtigster Hinweise beläuft sich auf 4. Diese Anzahl wurde nur von einem Teilnehmer/einer Teilnehmerin erreicht. Insgesamt zehn der 32 Probanden fixierten nicht einen der acht wichtigsten Hinweise, bevor sie ihre Daten angeben wollten. Die Ergebnisse bezüglich der Verteilung der Operationalisierung des tatsächlichen Verhaltens sind in Abbildung 13 dargestellt. Sowohl der durchgeführte Kolmogorov-Smirnov-Test (p=.004), als auch der Shapiro-Wilk-Test (p=.001) kommen zu dem Ergebnis, dass keine Normalverteilung der Werte vorliegt.

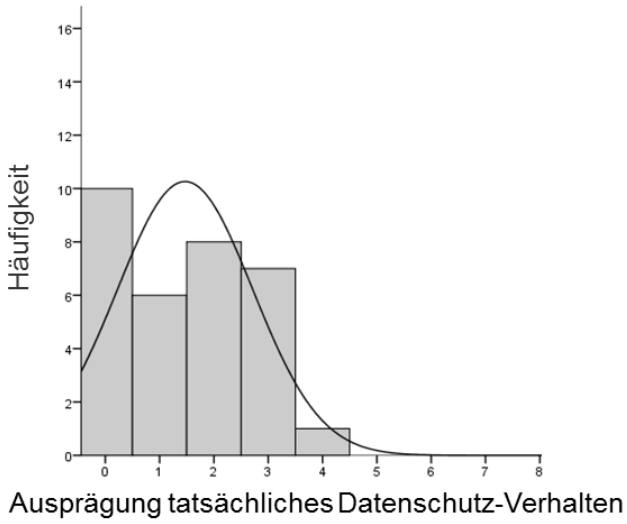


Abbildung 13. Verteilung des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping auf Basis der Ergebnisse der Explorationsstudie.

4.4 Ergebnisse bezüglich des Potentials der Prädiktoren

Mit 32 verbliebenen Datensätzen ist die vorhandene Stichprobe für die meisten an dieser Stelle interessanten Analyseverfahren zu gering. Erschwerend kommt hinzu, dass nur eine der erhaltenen Variablen normalverteilt vorliegt. Die meisten in Kapitel 4.1 aus der Forschungsfrage 2 abgeleiteten Hypothesen lassen sich aber mit Hilfe des sogenannten Mann-Whitney-U-Testes (Mann & Whitney, 1947) überprüfen. Dabei handelt es sich um einen Signifikanztest, mit dessen Hilfe zwei unabhängige Stichproben unabhängig von ihrer Verteilung verglichen werden können (Bortz, 2005). Die Variablen *Bildung*, *Einkommen* und *Nutzungshäufigkeit* werden aufgrund ihrer schmalen Verteilungen nicht weiter untersucht. Die restlichen zu untersuchenden Variablen müssen für die weitere Analyse zunächst in entsprechende Gruppen unterteilt werden. Dies geschieht im Falle von stetigen Variablen wie z. B. *Alter*, *objektiven* oder *subjektivem Wissen,* indem Grenzen, eine Standardabweichung über und unter dem Mittelwert gezogen werden. Die außerhalb dieser Grenzen liegenden „Randgruppen" werden dann miteinander verglichen. Dies entspricht einer Einteilung, die von Weber et al. (2002) vorgenommen wurde. Im Falle von diskreten Variablen wie *Einkommen* oder *Bildung* werden jeweils die am weitesten entfernt voneinander liegenden Ausprägungen verglichen, in die Versuchspersonen eingeordnet werden konnten. Die Auswahl der Alternativhypothesen, deren entsprechenden Nullhypothesen aufgrund signifikanter Unterschiede zwischen den Gruppen verworfen werden konnten, ist in Tabelle 15 dargestellt.

Tabelle 15. Ergebnisse der signifikanten Mann-Whitney-U-Tests und eines t-Test (inklusive der Gruppeneinteilung und der entsprechenden Mittelwerte (MW)), die zum Verwerfen der entsprechenden Nullhypothesen geführt haben.

Hypothese	**Ergebnis**	**Signifikanz**	
Alter_12	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich der Wahrscheinlichkeit etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen (MW jünger als 17,35 Jahre =48,75; MW älter als 34,23 Jahre=36).	U = 2,000	p=.086
Geschlecht_1	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich des tatsächlichen Wissens (MW weiblich=4,45; MW männlich=7,23).	U = 28,000	p=.000
Geschlecht_2	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich des wahrgenommenen Wissens (MW weiblich=15,09; MW männlich=26,06).	U = 52,500	p=.004
Geschlecht_4	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich des wahrgenommenen Risikos im Internet Daten anzugeben, ohne die Datenschutzerklärungen angeschaut zu haben (MW weiblich=35,89; MW männlich=28,50).	U = 73,500	p=.046
Geschlecht_5	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich des wahrgenommenen Risikos vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt (MW weiblich=42,06; MW männlich=36,29).	U = 70,500	p=.034

N.-dauer_9	Die Gruppe der Nutzer, die das Internet seit 3 bis unter 7 Jahren nutzt unterscheidet sich von der Gruppe, die das Internet seit mehr als 10 Jahren nutzt bezüglich der Wahrscheinlichkeit etwas online zu kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen (MW 3-7 Jahre=48,50; MW mehr als 10 Jahre=40,25).	U = 18,000	p=.017
N.-dauer_11	Die Gruppe der Nutzer, die das Internet seit 3 bis unter 7 Jahren nutzt unterscheidet sich von der Gruppe, die das Internet seit mehr als 10 Jahren nutzt bezüglich der Wahrscheinlichkeit vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt (MW 3-7 Jahre=33,88; MW mehr als 10 Jahre=23,83).	U = 26,000	p=.094
tats.Wissen_1	Die Gruppe der Nutzer mit niedrigem Score für tatsächliches Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für tatsächliches Wissens bezüglich des wahrgenommenen Wissen (MW tats. Wissen<3,52=13,19; MW tats. Wissen>7,82=29,07).	U = 5,000	p=.011
wahrg.Wissen_9	Die Gruppe der Nutzer mit niedrigem Score für wahrgenommenes Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für wahrgenommenes Wissen bezüglich der Wahrscheinlichkeit vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt (MW wahrg. Wissen<9,26=32,40; MW wahrg. Wissen>30,52=18,33).	t(9)= -27,151	p=.066
Risiko_1	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt, unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich des tatsächlichen Wissens (MW Risiko<31,944=6,92; MW Risiko>47,116=4,67).	U = 6,000	p=.056
Risiko_8	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko im Internet Daten anzugeben, ohne die Datenschutzerklärungen angeschaut zu haben, unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich des erwarteten Nutzens im Internet Daten anzugeben, ohne die Datenschutzerklärungen angeschaut zu haben(MW Risiko<21,257=21,0; MW Risiko>44,063=4,8).	U = 1,000	p=.032
Nutzen_1	Die Gruppe der Nutzer mit einem niedrigen erwarteten Nutzen etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen, unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen erwarteten Nutzen bezüglich der Wahrscheinlichkeit etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen (MW Nutzen<5,856=28,43; MW Nutzen>28,484=48,33).	U = 1,000	p=.033

Nutzen_6	Die Gruppe der Nutzer mit einem niedrigen erwarteten Nutzen vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt, unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen erwarteten Nutzen bezüglich des tatsächlichen Verhaltens "vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt" (MW Nutzen<1,091=0,67; MW Nutzen>19,949=0,0).	U = 5,000	p=.061

Es zeigt sich, dass von den demographischen Faktoren das *Alter*, das *Geschlecht* und die *Nutzungsdauer* zu Unterschieden bezüglich des *objektiven Wissens*, der *Wahrscheinlichkeit für Risikoverhalten* und des *wahrgenommenen Risikos* führen. So geben die jüngeren Teilnehmer eine höhere Wahrscheinlichkeit an, dass sie etwas online kaufen, ohne vorher die AGB gelesen zu haben. Männer und Frauen unterscheiden sich sowohl im objektiven, als auch im subjektiven Wissen. In beiden Fällen ergab sich bei der Gruppe der Männer ein höheres Wissen. Dies entspricht auch Hypothese *tats.Wissen_1*, deren Ergebnis besagt, dass ein besseres Ergebnis bezüglich des objektiven Wissens auch mit einem höheren subjektiven Wissen einhergeht. Die Gruppe der Frauen nimmt dagegen ein höheres Risiko wahr, Daten anzugeben, ohne die Datenschutzerklärungen gelesen zu haben, bzw. ohne überprüft zu haben, ob es sich um eine verschlüsselte Verbindung handelt.
Die Gruppe der Probanden mit geringeren subjektivem Wissen gibt eine höhere Wahrscheinlichkeit dafür an, nicht darauf zu achten, ob die Verbindung verschlüsselt ist. Diejenigen, die das Risiko, das sich aus diesem Verhalten ergibt, geringer einschätzen als andere, sind dagegen die, die über ein besseres objektives Wissen verfügen. Entsprechend den Erwartungen empfindet diese Gruppe der Probanden, das Risiko, welches sich ergibt, wenn Daten angegeben werden, ohne dass die Datenschutzerklärung gelesen wurde, als geringer und geben, diesbezüglich einen höheren erwarteten Nutzen an. An der Stelle sind der Aufwand und die Zeitersparnis eine denkbare Erklärung. Dementsprechend gibt die Gruppe, die geringeren Nutzen darin sieht, etwas zu kaufen, ohne die AGB gelesen zu haben, auch eine geringere Wahrscheinlichkeit dafür an, genau dies zu tun. Interessanterweise zeigte die Gruppe der Probanden, die einen geringeren Nutzen dafür angab, sich nicht zu versichern, dass es sich um eine verschlüsselte Verbindung handelt, das Verhalten auch öfter. Während aus diesen sechs Personen vier Hinweise auf Verschlüsselung (*https* und/oder *EV-SSL-Zertifikat*) fixierten, tat das aus der Gruppe, die den Nutzen hoch einschätzte das nicht zu tun, niemand. Bezüglich der Vorhersage des tatsächlichen Verhaltens zeigten sich darüber keine nennenswerten Zusammenhänge

4.5 Diskussion der Explorationsstudie

Auf Basis des in Kapitel 3 erarbeiteten Vorgehens zur empirischen Erfassung von Datenschutz-Verhalten beim Onlineshopping wurde eine Explorationsstudie mit 50 Probanden und Probandinnen durchgeführt. Diese soll an dieser Stelle diskutiert werden. Eine umfassende Diskussion des gesamten Vorgehens im Rahmen dieser Arbeit folgt zusätzlich in Kapitel 6.
Der für die Explorationsstudie verwendete Versuchsaufbau sowie der Versuchsablauf bieten auch im Anschluss an die Durchführung keinen Grund für Kritik. Dies gilt nicht für alle verwendeten Methoden. In Bezug auf die verwendeten Fragbögen ist zu sagen, dass diese zwar mit Hilfe eines Online-Befragungs-Tools erarbeitet worden waren, aber im Rahmen der Laborstudie ausgefüllt wurden. Dies bot die Möglichkeit, dass die Teilnehmer und Teilnehmerinnen bei Unklarheiten während der Beantwortung

Fragen an die Versuchsleiterin stellen konnten. Hier wurden zwar vereinzelt Fragen gestellt, es konnte aber keine Systematik festgestellt werden, die dazu führen würde, dass ein häufig nicht oder missverstandenes Item kritisch hinterfragt werden müsste. Die Verwendung der Online-Befragungssoftware bot den großen Vorteil, dass so die Daten direkt digital vorlagen und nicht zunächst händisch übertragen werden mussten, wie das bei einem Paper-Pencil-Test der Fall ist (Döring & Bortz, 2016). Bezüglich der Aufgabe lässt sich sagen, dass deren Instruktion (siehe Anhang C) dazu geführt hat, dass ein nicht unwesentlicher Teil der Probanden nicht wirklich verstanden hatte, dass wirklich ein Produkt unter Zuhilfenahme der eigenen Daten gekauft werden sollte. Dies führte zu einer relativ großen Anzahl an Teilnehmern, deren Daten für die Berechnung des tatsächlichen Verhaltens nicht einbezogen werden konnten. Die Teilnehmer, welche die Aufgabe vollständig und zufriedenstellend bearbeiteten, erweckten den Eindruck, dass sie nicht durch die Blickbewegung wesentlich abgelenkt oder generell beeinflusst waren. Dies wird der Verwendung des Remote Eye-Trackers zugeschrieben, welcher verhindert, dass wie bei anderen Systemen Brillen oder andere Apparaturen am Kopf der Probanden getragen werden müssen. Scheinbar fiel es den Teilnehmern auch nicht schwer, während der gesamten Aufgabenbearbeitung in der Reichweite des Eye-Trackers zu verbleiben, denn die Versuchsleiterin musste nur sehr selten an die richtige Sitzposition erinnern. Generell wird die Verwendung des Eye-Trackers als vielversprechende Methode angesehen. So gelang es, das Blickverhalten der Versuchspersonen aufzuzeichnen und interessante Ergebnisse bezüglich der Betrachtung der verschiedenen AOI zu erhalten. Andererseits erwies sich die Auswertung der Daten als sehr umfangreich und aufwändig. Dies ergab sich vor allem aus der Anforderung, dass die Teilnehmer sich im Rahmen des Internets frei bewegen können sollten. So war es nicht möglich, die AOI auf einer Webseite zu legen und diese dann auf alle Probanden anzuwenden. Es mussten für jeden einzelnen Probanden, alle vorhandenen AOI, auf jeder der betrachteten Seiten des Webshops gelegt werden. Um den Aufwand wenigsten einigermaßen in Grenzen zu halten, wurde sich hierfür deshalb auf die Analyse des Webshops beschränkt, bei dem die Probanden bereit waren ihre Daten anzugeben. Dies kann damit begründet werden, dass die Informationssuche bezüglich der Vertrauenswürdigkeit eines Webshops in dem Moment als abgeschlossen betrachtet wird, in dem die Teilnehmer bereit sind, dort ihre Daten anzugeben.

Auch die Tatsache, dass bei einigen der Probanden deren Brille zu Fehlern bei der Blickerfassung führte, wird als kritisch angesehen. Mit anderen Brillen-Modellen funktionierte das Gerät problemlos. Dies war besonders ärgerlich, weil die Probleme erst im Rahmen der Kalibrierung auftreten. Zu diesem Zeitpunkt wurde der Großteil der verwendeten Fragebögen schon ausgefüllt. Ein Abbruch zu einem solch verhältnismäßig späten Zeitpunkt im Versuch ist sowohl für den Versuchsleiter/die Versuchsleiterin, als auch den teilnehmenden Probanden/die teilnehmende Probandin sehr ärgerlich.

Bei der erhaltenen Stichprobe handelt es sich dadurch, dass zwar öffentlich viele potentielle Teilnehmer angesprochen wurden, aber keine mathematische definierte Zufallsauswahl stattgefunden hat, um eine Gelegenheits-, bzw. Selbstselektionsstichprobe (Döring & Bortz, 2016).

Diesbezüglich ist anzumerken, dass das anvisierte Ziel, eine möglichst breite Verteilung der unterschiedlichen demographischen Attribute abbilden zu können, nicht in Bezug auf alle Variablen erreicht wurde. Am ehesten entsprechen diesem Ziel die Variablen Alter und Geschlecht. Bildung und Einkommen weisen dagegen starke Verzerrungen auf. So stellen sich die Teilnehmer insgesamt als hoch gebildet, aber tendenziell wenig verdienend dar. Dies lässt den Schluss zu, dass es sich bei vielen von ihnen dann doch um Studenten, bzw. Berufsanfänger handelt. Die Variable der Interneterfahrung Nutzungshäufigkeit eignet sich darüber hinaus nicht, um die Versuchsteilnehmer daran zu unterscheiden. So verwenden nur zwei der Probanden und Probandinnen das Internet nicht täglich. Bezüglich der Variable Nutzungsdauer verteilen sich die Angaben auf immerhin drei der vier möglichen

Antwortkategorien. Zu dieser Zeit findet man allerdings wohl kaum erwachsene Menschen, die das Internet erst seit weniger als 3 Jahren nutzen. Es ist davon auszugehen, dass diese Variable im Laufe der Zeit immer mehr an Unterscheidungskraft verlieren wird. Dies zeigt sich auch in den Ergebnissen der mehrmals im Jahr erhobenen „internet facts“ der Arbeitsgemeinschaft Online Forschung e.V. Während der Anteil der Nutzer, die das Internet seit weniger als 3 Jahren verwenden, im Jahr der Erhebung der Explorationsstudie noch zusammengerechnet bei 11,4% lag (Arbeitsgemeinschaft Online Forschung e.V., 2013), lag er im Jahr der im Folgenden beschriebenen Validierungsstudie bei nur noch 7,5% (Arbeitsgemeinschaft Online Forschung e.V., 2015).

Neben der Erfassung dessen, was die Teilnehmer der Studie meinen zu wissen, wurde in dieser Studie im Gegensatz zu den meisten anderen Studien (Hargittai, 2005; van Deursen & van Dijk, 2010) mit Hilfe eines eigens konzipierten Wissenstests auch das tatsächliche Wissen erfasst. Die erhaltenen Verteilungen diesbezüglich und die der Variable Besitz sehen sehr zufriedenstellend aus. So ergab sich für die Variablen, die sich aus dem Wissenstest ergeben, jeweils eine Normalverteilung der erhaltenen Werte.

Bezüglich der Auswertung der Blickbewegungen zeigte sich, dass der Preis, das Produktbild und die Produktbeschreibung am häufigsten betrachtet wurden, was der vordergründigen Aufgabe des Onlineshoppings geschuldet ist. Aber auch datenschutzrelevante AOI, wie die AGB oder der Unternehmensname wurden vergleichsweise häufig betrachtet. Die Berechnung des Wertes für das tatsächliche Datenschutz-Verhalten beim Onlineshopping kommt aber zu dem Schluss, dass sich die Probanden nur sehr eingeschränkt vorsichtig diesbezüglich verhalten. So überprüfte nur eine Person immerhin vier der acht wichtigsten Hinweise, bevor er oder sie bereit war, die persönlichen Daten anzugeben. Alle anderen Teilnehmer überprüften weniger und 10 von ihnen sogar gar keinen Hinweis.

Bezüglich der überprüften Hypothesen zeigten sich zwar nur wenige, aber interessante Ergebnisse. So konnte nachgewiesen werden, dass sowohl das objektive als auch das subjektive Wissen der männlichen Teilnehmer höher war als das der weiblichen. Möglicherweise damit einhergehend, nehmen die Probandinnen ein höheres Risiko bezüglich zwei der drei risikoreichen Verhalten wahr als die Probanden. Unterschiede im Wissen, die sich aus Alter oder Bildung ergeben, wie sie von van Deursen und van Dijk (2010) gefunden wurden, konnten im Rahmen dieser Studie nicht nachgewiesen werden. Dies gelang immerhin teilweise mit den erwarteten Zusammenhängen zwischen dem wahrgenommenen Risiko und dem erwarteten Nutzen, bzw. dem erwarteten Nutzen und der Wahrscheinlichkeit für Verhalten.

Die im Rahmen der Explorationsstudie erhaltenen Ergebnisse werden im Folgenden verwendet, um das in Kapitel 4.1 erarbeitete Arbeitsmodell zu verkleinern und somit für kleinere Stichproben überprüfbar zu machen. Die Anpassung des Modells sowie die Überprüfung dessen und deren Ergebnisse sind im folgenden Kapitel 5 dargestellt.

5 Vorhersage von Datenschutz-Verhalten beim Onlineshopping

In Kapitel 4.1 wurde ein Arbeitsmodell auf Basis der in Kapitel 2 dargestellten Erkenntnisse aufgestellt. Dieses wurde mit Hilfe der in Kapitel 4.2 vorgestellten Explorationsstudie in einem ersten Schritt auf vielversprechende Prädiktoren untersucht. Auf Basis der in Kapitel 4.3 und 4.4 dargestellten Ergebnisse wird das erste Arbeitsmodell in Kapitel 5.1 in zwei kleinere überprüfbare Modelle aufgeteilt. Beide dieser Modelle sollen im Folgenden validiert werden. Die dafür durchgeführte Validierungsstudie wird in Kapitel 5.2 dargestellt. Die Ergebnisse dieser sind Inhalt von Kapitel 5.3 und speziell die Ergebnisse der Vorhersage von Kapitel 5.4. Den Abschluss dieses Kapitels bilden die validierten Modelle in Kapitel 5.5.

5.1 Anpassung des Arbeitsmodells

Bezugnehmend auf die Ergebnisse der Hypothesentestung in Kapitel 4.4 wird das in Kapitel 4.1 vorgestellte Arbeitsmodell an dieser Stelle angepasst. Die Anpassung wird mit Hilfe der Validierungsstudie, die in Kapitel 5.2 vorgestellt und beschrieben ist, überprüft. Da diese Validierungsstudie inhaltlich sowie vom Aufbau her der bereits vorgestellten Explorationsstudie entspricht, gelten entsprechend auch die gleichen Einschränkungen, die sich hauptsächlich auf die kleine Anzahl Probanden bezieht. Mit Hilfe von ca. 50 Versuchspersonen ist die Auswahl geeigneter Methoden zur Testung ganzer Modelle nur sehr gering. Eine „Daumenregel“ zur Modelltestung besagt, dass auf jeden Parameter des Modells mindestens 5-10 Versuchspersonen kommen müssen (Muthén & Muthén, 2002). Zwar konnten Muthen und Muthen (2002) zeigen, dass generelle Angaben dazu kaum möglich sind. Trotzdem wird an dieser Stelle das umfangreiche Arbeitsmodell aus Kapitel 4.1 in kleinere und somit überprüfbare Modelle unterteilt. Das Ziel bleibt in jedem der Fälle die Vorhersage tatsächlichen Verhaltens.

Aus den Mann-Whitney-U-Tests in Kapitel 4.4 ergaben sich die Faktoren *Alter*, *Geschlecht*, *Nutzungsdauer*, sowie *subjektives* und *objektives Wissen* als aussagekräftige Personenfaktoren. Bezüglich der *Nutzungsdauer* gibt es zwei Gründe, die gegen eine weitere Verwendung dieser Variable sprechen. Zum einen wird ein Zusammenhang zwischen der *Nutzungsdauer* und dem *Alter* vermutet, der allerdings aufgrund der schmalen Verteilung nicht mit den Daten dieser Studie überprüft werden konnte. Darüber hinaus wird davon ausgegangen, dass sich durch die Generation der „Digital Natives“, die schon im Kindesalter mit dem Internet in Berührung kommt, eine Gruppe, die das Internet seit weniger als 3 Jahren nutzt, in Zukunft kaum noch finden lässt (siehe Kapitel 4.5). Im Rahmen der Anpassung des Modells wird deshalb auf die weitere Verwendung dieses Faktors verzichtet. Die anderen vier Faktoren bilden die Prädiktoren, deren Einfluss auf das tatsächliche Datenschutz-Verhalten weiter untersucht werden soll. Es ergibt sich somit ein Modell, welches in Abbildung 14 dargestellt ist.

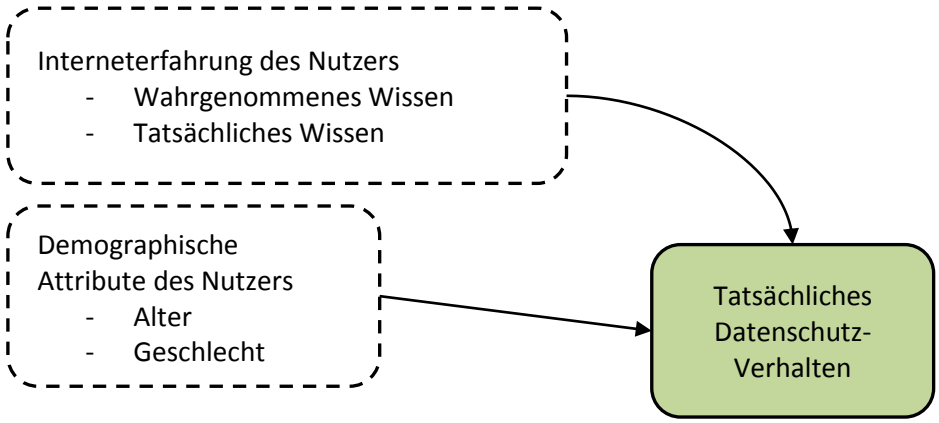


Abbildung 14. Angepasstes Modell zur Vorhersage des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping.

Darüber hinaus zeigten sich auch die Variablen des *wahrgenommenen Risikos*, des *erwarteten Nutzens* und der *angegebenen Wahrscheinlichkeit* als aussichtsreiche Prädiktoren für die entsprechende risikoreiche Handlung. Aus diesem Grund soll mit Hilfe der Daten der Validierungsstudie auch ein weiteres Modell im Ganzen überprüft werden. Da es sich im Rahmen der Gewichtungsstudie (Kapitel 3.2.2) ergab, dass der Hinweis *Informationen zu Datenschutz/Datensicherheit* von den Experten am häufigsten zu den wichtigsten Hinweisen gezählt wurde, soll insbesondere dessen Überprüfung analysiert werden. Das sich ergebende Modell ist in Abbildungen 15 dargestellt.

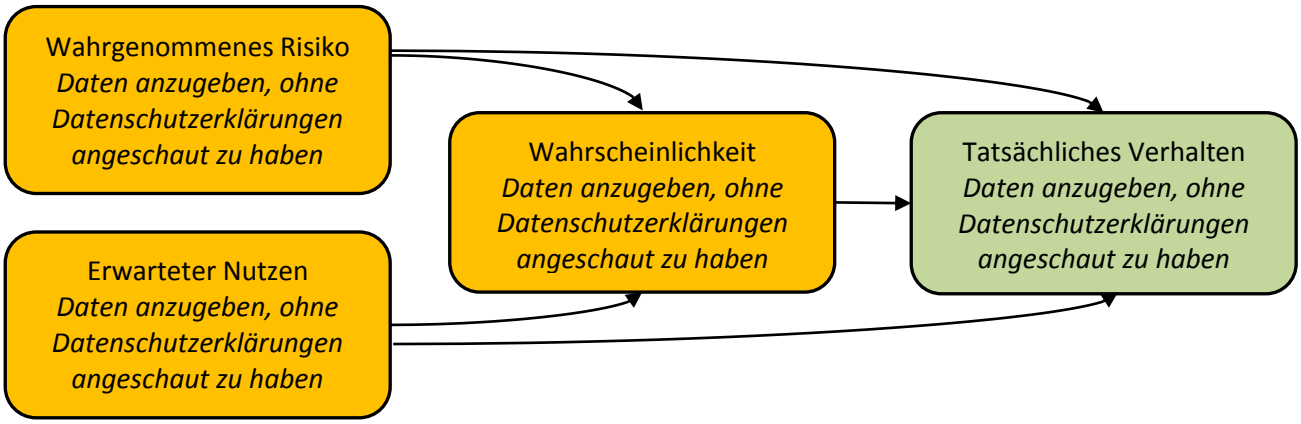


Abbildung 15. Modell zur Vorhersage der Handlung *im Internet Daten anzugeben, ohne die Datenschutzerklärungen angeschaut zu haben*, mit Hilfe des entsprechenden wahrgenommenen Risikos, des erwarteten Nutzens und der angegebenen Wahrscheinlichkeit.

5.2 Vorgehen Validierungsstudie

Die Erhebung bezüglich der hier beschriebenen Validierungsstudie fand im Zeitraum zwischen dem 7. Juli 2015 und dem 15. Januar 2016 in den gleichen Räumlichkeiten statt, die auch schon zur Erhebung der Explorationsstudie genutzt wurden. Es nahmen 43 Probanden an der Studie teil. Um die Ergebnisse so vergleichbar wie möglich zu halten, wurde darauf geachtet, möglichst die gleichen Bedingungen

herzustellen. Erfahrungen aus der Explorationsstudie führten trotzdem zu einigen Anpassungen, die im folgenden Kapitel dargestellt werden.

5.2.1 Anpassungen der Studie

Ziel der Validierungsstudie war die Reproduktion der bereits im Rahmen der Explorationsstudie erlangten Erkenntnisse. Aus diesem Grund war es notwendig, dass das Versuchsdesign möglichst wenig abwich. Die einzige Änderung bezüglich der verwendeten Technik bestand darin, dass zur Bearbeitung der Fragebögen ein zusätzlicher Laptop verwendet wurde. Dies führte zwar dazu, dass die Probanden zweimal den Platz wechseln mussten. Bei einer Dauer der Studie von ca. 1,5 Std. je Proband wurde etwas zusätzliche Bewegung aber als Vorteil gesehen. Abbildung 16 zeigt den Aufbau im Rahmen der Validierungsstudie.

Abbildung 16. Aufbau im Rahmen der Validierungsstudie (aus Becker, 2015; Dörner, 2015).

Da sich das Alter der Probanden trotz Einschränkungen in der Verteilung als vielversprechender Faktor erwies, sollte bei der Anwerbung der Probanden der zweiten Studie auf eine breitere Altersverteilung geachtet werden. Die einzelnen Kategorien bezüglich des Besitzes internetfähiger Geräte wurden um die Kategorie *Smart TV* ergänzt. Erwähnt sei, dass bei der Verwendung der Visuellen Analog-Skala im Falle der Validierungsstudie nicht erneut Werte von 1-50, sondern von 1-100 der Skala hinterlegt wurden. Da die hinterlegten Werte für die Probanden jeweils nicht sichtbar waren, ergeben sich daraus keinerlei Schwierigkeiten.

Im Rahmen der Explorationsstudie ergab es sich außerdem, dass die Daten einiger Teilnehmer nicht für die eigentliche Analyse verwendet werden konnten, da sie die Aufgabe, sich ein Produkt mit Hilfe ihrer eigenen personenbezogenen Daten und ihrem eigenen Geld zu kaufen, nicht zufriedenstellend bearbeiteten. Einer der Gründe hierfür wurde darin gesehen, dass die Aufgabenstellung die Verwendung der eigenen Daten und des eigenen Geldes nicht deutlich genug machte. Aus diesem Grund wurde die Aufgabenstellung mit dem zusätzlichen Hinweis versehen, dass die in Aussicht gestellte Aufwandsentschädigung verwendet werden sollte, um online das Produkt zu erwerben. Bis auf die Person der Versuchsleitung, die in der Explorationsstudie weiblich und in der Validierungsstudie männlich war, wurden alle Bedingungen darüber hinaus gleich gehalten.

5.3 Ergebnisse Validierungsstudie

Ein Unterschied zur vorangegangenen Explorationsstudie schlägt sich direkt in den Daten nieder. Im Rahmen der Validierungsstudie gibt es nur zwei Probanden, deren Daten nicht verwendet werden können, weil sie nicht bereit waren, diese zum Kauf eines Produktes im Rahmen der Studie anzugeben. Aufgrund der geänderten Aufgabenstellung war scheinbar allen Probanden klar, dass sie ihre eigenen Daten verwenden sollten, so dass niemand aufgrund nicht zufriedenstellender Aufgabenbearbeitung ausfiel. Im Folgenden werden ausschließlich die Daten dieser verbleibenden 41 Probanden ausgewertet. Auf eine zusätzliche Darstellung der deskriptiven Daten inklusive der zwei ausgeschlossenen Datensätze wird an dieser Stelle verzichtet.
Obwohl das in Kapitel 4.1 erstellte Arbeitsmodell in Kapitel 5.1 auf eine Auswahl von Variablen reduziert wurde, wurden alle Faktoren des ursprünglichen Modells im Rahmen der Validierungsstudie erfasst. Im Zuge der deskriptiven Beschreibung der Stichprobe werden diese deshalb verwendet, auch wenn sie nicht in die nachfolgenden Modelle einfließen. Tabelle 16 fasst alle deskriptiven Ergebnisse der Validierungsstudie zusammen, die folgend in den Kapiteln 5.3.1-5.3.5 beschrieben werden. Tests auf Normalverteilung kamen zu dem Ergebnis, dass nur die beiden Variablen zu objektivem (Shapiro-Wilk-Test $p=.695$) und subjektivem Wissen (Shapiro-Wilk-Test $p=.076$) einen Verlauf aufweisen, der einer Normalverteilung folgt.

Tabelle 16. Deskriptive Ergebnisse der Validierungsstudie.

n		41
Alter		22-68 (MW = 40,69; SD = 15,56)
Geschlecht	männlich	16 (39%)
	weiblich	25 (61%)
Bildung	"Noch Schüler"	
	"Schule beendet ohne Abschluss"	
	"Volks-, Hauptschulabschluss"	1 (2,4%)
	"Mittlere Reife, Realschul- oder gleichwertiger Abschluss"	1 (2,4%)
	"Abgeschlossene Lehre"	1 (2,4%)
	"Fachabitur, Fachhochschulreife"	3 (7,3%)
	"Abitur, Hochschulreife"	14 (34,1%)
	"Fachhochschul-/Hochschulabschluss"	21 (51,2%)

Einkommen	"nicht beantwortet"	1 (2,4%)
	"unter 1500€"	19 (46,3%)
	"1500€ bis unter 2000€"	5 (12,2%)
	"2000€ bis unter 2500€"	1 (2,4%)
	"2500€ bis unter 3000€"	3 (7,3%)
	"3000€ bis unter 3500€"	3 (7,3%)
	"3500€ bis unter 4000€"	
	"4000€ bis unter 4500€"	3 (7,3%)
	"4500€ bis unter 5000€"	1 (2,4%)
	"5000€ und mehr"	5 (12,2%)
Nutzungshäufigkeit	"täglich"	38 (92,7%)
	"mehrmals pro Woche"	2 (4,9%)
	"ein paar Mal pro Monat"	1 (2,4%)
	"seltener"	
Nutzungsdauer	"weniger als 3 Jahre"	
	"3 bis unter 7 Jahren"	
	"7 bis unter 10 Jahren"	11 (26,8%)
	"mehr als 10 Jahren"	30 (73,2%)
Besitz	Desktop-PC	20 (48,8%)
	Laptop/Notebook	36 (87,8%)
	Tablet-PC	14 (34,1%)
	Smartphone/Internetfähiges Telefon (z. B. iPhone, BlackBerry,…)	37 (90,2%)
	Spielekonsole (z. B. XBOX, Playstation, Game Cube,…)	4 (9,8%)
	Smart TV	11 (26,8%)
	"keines von diesen"	
Besitz gesamt		1-6 (MW=2,98; SD=1,129)
Wahrgenommenes Wissen		4,67-92 (MW = 37,67; SD = 22,45)
Tatsächliches Wissen		2-9,50 (MW = 5,74; SD = 1,84)
Tatsächliches Verhalten		0-4 (MW = 1,20; SD = 1,08)
Wahrgenommenes Risiko	AGB_Etwas online kaufen, ohne vorher die AGB zu lesen	1-100 (MW = 58,85; SD = 26,67)
	DSErkl_Daten anzugeben, ohne Datenschutzerklärungen angeschaut zu haben	20-100 (MW = 70,32; SD = 23,92)
	vVerb_Vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt	12-100 (MW = 78,10; SD = 23,12)

Erwarteter Nutzen	AGB_Etwas online kaufen, ohne vorher die AGB zu lesen	1-100 (MW = 37,63; SD = 29,84)
	DSErkl_Daten anzugeben, ohne Datenschutzerklärungen angeschaut zu haben	1-90 (MW = 37,61; SD = 27,57)
	vVerb_Vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt	1-90 (MW = 28,10; SD = 25,59)
Wahrscheinlichkeit	AGB_Etwas online kaufen, ohne vorher die AGB zu lesen	1-100 (MW =57,20 SD = 36,41)
	DSErkl_Daten anzugeben, ohne Datenschutzerklärungen angeschaut zu haben	1-100 (MW =57,90 SD = 33,58)
	vVerb_Vertrauliche Daten anzugeben, ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt	1-100 (MW =43,17; SD = 36,67)

5.3.1 Ergebnisse bezüglich der demographischen Attribute

Das Alter der Teilnehmer reichte von 22 bis 68 Jahren mit einem Mittelwert von 40,69 und einer Standardabweichung von 15,56. Die Aufteilung der Geschlechter zeigte sich mit 25 Teilnehmerinnen (61%) und 16 Teilnehmern (39%) als nicht völlig ausgeglichen. Bezüglich der Bildung und des Haushaltsnettoeinkommens ergaben sich in diesem Fall etwas homogenere Verteilungen als bei der Explorationsstudie. Diese sind in Abbildung 17 und Abbildung 18 zu sehen.

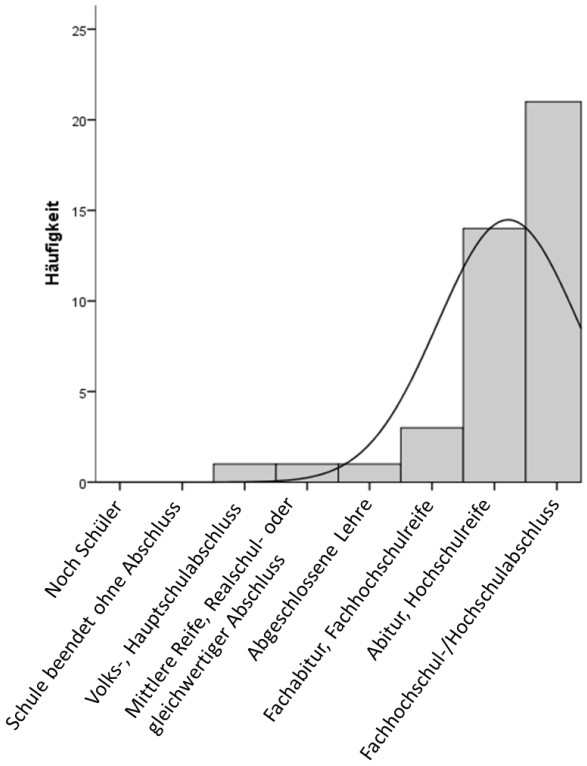


Abbildung 17. Angegebener höchster Bildungsabschluss der Probanden der Validierungsstudie.

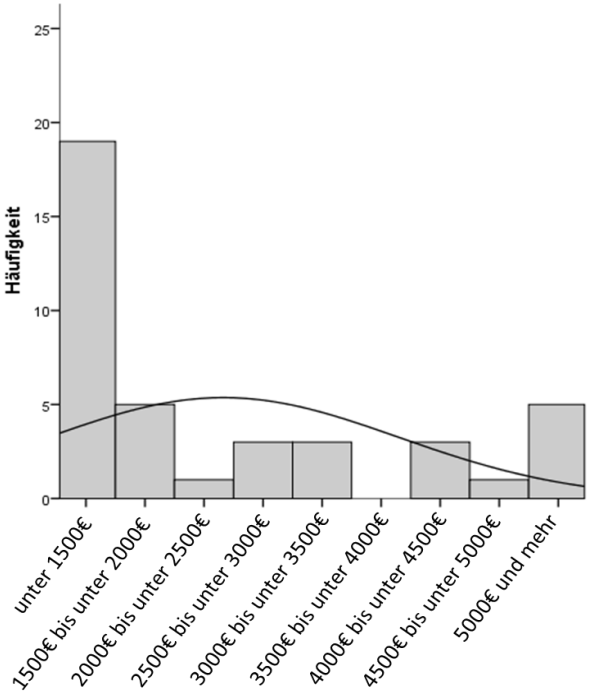


Abbildung 18. Angegebenes Haushaltsnettoeinkommen der Probanden der Validierungsstudie.

5.3.2 Ergebnisse bezüglich der Erfahrung

In Bezug auf die Nutzungshäufigkeit wurde in diesem Falle einmal (2,4%) die Kategorie „ein paar Mal pro Monat“ besetzt. Zwei der Probanden (4,9%) nutzen das Internet „mehrmals pro Woche“ und 38 (92,7%) „täglich“.
Einen Desktop-PC besitzen 20 der Probanden (48,8%), einen Laptop, bzw. ein Notebook 36 (87,8%) und einen Tablet-PC 14 Probanden (34,1%). Von den 41 Teilnehmern besaßen zu diesem Zeitpunkt 37 (90,2%) ein internetfähiges Telefon und 4 (9,8%) eine Spielekonsole. Die neu hinzugekommene Besitzkategorie Smart TV nannten 11 Personen (26,8%) ihr eigen.
Im Vergleich zur Explorationsstudie haben sich somit der Anteil Probanden, die einen Desktop PC und der, die einen Tablet PC besitzen, verdoppelt. Die anderen Anteile sind nahezu gleich in beiden Studien.

In Bezug auf das objektive Wissen erreichten die Teilnehmer der Validierungsstudie Punkte von 2 bis 9,50. Der Mittelwert lag bei 5,74 und die Standardabweichung betrug 1,84. Diese Werte entsprechen in etwa denen, die bereits in der Explorationsstudie erreicht wurden. Beim subjektiven Wissen ergaben sich Werte zwischen 4,67 und 92, was sich aus der in dieser Studie verwendeten Skala von 1-100 ergibt. Der Mittelwert für das subjektive Wissen lag bei 37,66 und die Standardabweichung betrug 22,451. Die Reliabilität dieser zusammengesetzten Variablen ist mit einem Cronbach´s Alpha von .761 ausreichend.

5.3.3 Ergebnisse bezüglich der Einschätzungen der Risikosituationen

Die Einschätzungen der risikoreichen Handlung unterscheiden sich augenscheinlich in ihren Ergebnissen bezüglich des wahrgenommenen Risikos, des erwarteten Nutzens und der angegebenen Wahrscheinlichkeit in ihrer Tendenz kaum von denen der Explorationsstudie. Auch in der Validierungsstudie wird das Risiko als eher hoch wahrgenommen (MW AGB=58,85; MW DSErkl=70,32 und MW vVerb=78,10 auf Skala 0=„überhaupt kein Risiko“ bis 100=„sehr hohes Risiko“) und der Nutzen vergleichsweise gering (MW AGB=37,63; MW DSErkl= 37,61 und MW vVerb=28,10 auf Skala 0=„gar keinen Nutzen“ bis 100=„großen Nutzen“). Daraus ergibt sich in allen Fällen eine mittlere Wahrscheinlichkeit (MW AGB=57,20; MW DSErkl=57,90 und MW vVerb=43,17 auf Skala 0=„sehr unwahrscheinlich“ bis 100=„sehr wahrscheinlich“) dafür, das Verhalten zu zeigen.

5.3.4 Ergebnisse bezüglich der Blickbewegung

Aus Gründen des immens hohen Aufwandes bezüglich der Auswertung der Blickbewegungen wird sich bei der Auswertung der Validierungsstudie auf die Hinweise beschränkt, die sich im Rahmen der Gewichtungsstudie als die wichtigsten ergaben. Zusätzlich werden die Hinweise analysiert, die von den Probanden der Explorationsstudie am häufigsten fixiert wurden (*Preis*, *Produktbeschreibung* und *Produktbild*). Entsprechend zu Tabelle 14 in Kapitel 4.3.5 sind die Ergebnisse dieser Analyse in Tabelle 17 dargestellt.
In der ersten Spalte lässt sich erkennen, dass einzig der Hinweis *Shopname (URL)* auf allen 41 analysierten Seiten vorhanden war. Darüber hinaus gab es keinen Hinweis, der auf keiner der Seiten zu finden gewesen wäre. Von 13 Probanden insgesamt am häufigsten fixiert wurde auch der Hinweis *Shopname (URL)*. Dahinter folgt mit 11 Probanden der Hinweis *Gütesiegel*. Obwohl sie zu den wichtigsten Hinweisen gehören und auch vorhanden waren, wurden die Hinweise *Name & Anschrift des Anbieters*

und *Expertenbeurteilungen, Testberichte…* von keinem der Probanden fixiert. Der zweite Hinweis war mit 4 Webshops zwar zugegebenermaßen selten vorhanden, am Hinweis *EV-SSL Zertifikat* zeigt sich aber, dass dies nichts bedeuten muss. Obwohl nur auf insgesamt sechs Webshops vorhanden, wurde diese AOI immerhin in der Hälfte der Fälle auch fixiert. Ab der vierten Spalte zeigt sich die Tabelle nur wenig gefüllt. Dies begründet sich bei den Hinweisen *Name & Anschrift des Anbieters* und *Expertenbeurteilungen, Testberichte…* eben darin, dass gar keine Fixationen in diesen AOI stattgefunden haben. Bei den anderen Hinweisen wurde bereits in Kapitel 4.3.5 darauf hingewiesen, dass das Programm BeGaze keine Auswertung der entsprechenden Browserzeile unterstützte und diese Auswertung rein visuell vorgenommen werden musste. Dies führte aber nur zu der Information, ob eine Fixation in diesem Areal stattfand oder nicht. Dauern, Sequenzen und ähnliche Daten konnten auf diese Art aber nicht erfasst werden.

Tabelle 17. Ergebnisse der Validierungsstudie bezüglich der Blickbewegungsanalyse hinsichtlich der wichtigsten acht Hinweise und der Hinweise Preis, Produktbeschreibung und Produktbild (Vpn = Anzahl der Versuchspersonen, Fix. = Fixationen, NDwell Time = Normalized Dwell Time).

AOI	**Vorhanden**	**Vpn**	**Anzahl Fix.**	**Dauer Fix. [ms]**	**Rang**	**NDwell Time [ms/Coverage]**	**Revisits**
EV-SSL Zertifikat	6	3					
Expertenbeurteilungen, Testberichte, Awards…	4	0					
Gütesiegel	30	11	1,62	418,69	3,38	310956,75	0,54
https	40	6					
Infos zu DS	40	9	5,60	1619,95	2,50	320516,75	3,10
Kundenbeurteilungen des Shops	26	7	2,93	633,41	3,57	430400,27	1,50
Name & Anschrift des Anbieters	20	0					
Preis	39	33	2,03	663,84	3,15	1127983,51	0,84
Produktbeschreibung	40	35	8,27	2727,94	3,06	187500,73	1,67
Produktbild	40	37	7,97	2093,31	2,38	146118,80	2,83
Shopname (URL)	41	13					

5.3.5 Ergebnisse bezüglich des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping

Mit Hilfe der Analyse der Blickbewegungen wurde, entsprechend dem in Kapitel 4.3.6 vorgestellten Verfahren, auch im Rahmen der Validierungsstudie ein Wert für das tatsächliche Datenschutz-Verhalten eines jeden Probanden errechnet. Die Verteilung dieser Variable ist in Abbildung 19 dargestellt.

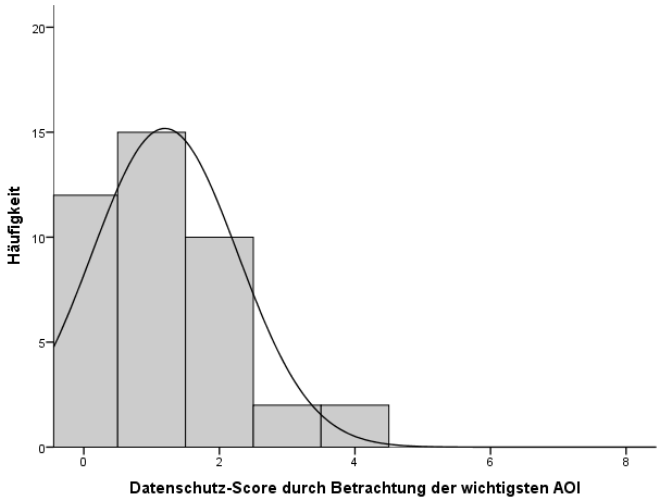


Abbildung 19. Verteilung des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping auf Basis der Ergebnisse der Validierungsstudie.

Auch hier ergab es sich, dass keiner der Probanden alle acht Hinweise im Vorfeld überprüfte. Wieder beläuft sich die höchste Anzahl überprüfter Hinweise auf 4. Diesmal wurde dieser Wert allerdings von zwei der Probanden erreicht. Insgesamt 12 Teilnehmer (29,3%) überprüften keinen einzigen der acht wichtigsten Hinweise, bevor sie bereit waren, ihre persönlichen Daten anzugeben. Wie zu erwarten kommen sowohl der Kolmogorov-Smirnov- als auch der Shapiro-Wilk-Test (in beiden Fällen $p=.000$) zu einem signifikanten Ergebnis, was besagt, dass keine Normalverteilung vorliegt.

5.4 Ergebnisse bezüglich der Vorhersage von Datenschutz-Verhalten

Um möglichst aussagekräftige Ergebnisse bezüglich der Modellüberprüfung zu erhalten, wurden an dieser Stelle die Daten beider vorangegangener Studien (Explorations- und Validierungsstudie) zusammengefügt. Dies ist möglich, da sich die beiden Studien in ihrer Durchführung nur unwesentlich unterschieden. Wichtige Faktoren dabei sind die Verwendung der gleichen Fragebögen, die gleichen zu bearbeitenden Aufgaben, standardisierte Versuchsbedingungen, wie z. B. schriftlich präsentierte Aufgaben und Anweisungen, bis hin zu gleichen Räumlichkeiten und Geräten. Es ergibt sich daraus eine Stichprobe, die sich aus 73 Datensätzen zusammensetzt. Tabelle 18 fasst die sich ergebende Stichprobe bezüglich der im Rahmen der folgenden Modellberechnung verwendeten Variablen noch einmal deskriptiv zusammen.

Tabelle 18. Deskriptive Daten der aggregierten Stichprobe.

Variable	Ausprägung	Beschreibung
Alter		19-68 Jahre; MW= 34,34 (SD=14,905)
Geschlecht	weiblich	43 (58,9%)
	männlich	30 (41,1%)
objektives Wissen		1,17 - 9,50 Punkte; MW=5,71 (SD=1,968)
subjektives Wissen		4,67 -92; MW=38,593 (SD=21,812)

Score Datenschutz-Verhalten	0	22 (30,1%)
	1	21 (28,8%)
	2	18 (24,7%)
	3	9 (12,3%)
	4	3 (4,1%)
wahrgenommenes Risiko		20 - 100; MW=68,12 (SD=23,412)
erwarteter Nutzen		1 - 90; MW=35,88 (SD=25,247)
Wahrscheinlichkeit		1 - 100; MW=62,74 (SD=30,841)
Informationen zu Datenschutz/Datensicherheit	angeschaut	19 (26%)
	nicht angeschaut	54 (74%)

Die deskriptive Beschreibung des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping nach zusammenlegen der Studien ist zusammengefasst in Tabelle 19 dargestellt.

Tabelle 19. Zusammenfassung der Ergebnisse der Blickbewegungsanalysen bezüglich der acht wichtigsten Hinweise.

AOI	**Vorhanden**	**Anzahl Probanden**
Infos zu DS	67	19
EV-SSL Zertifikat	16	4
Name & Anschrift Anbieter	44	3
https	72	10
Gütesiegel	51	16
Shopname (URL)	73	23
Expertenbeurteilungen, Testberichte, Awards…	18	5
Kundenbeurteilungen des Shops	41	15

Als erstes soll nun das in Kapitel 4.4 beschriebene angepasste Modell zur Vorhersage von tatsächlichem Datenschutz-Verhalten beim Onlineshopping berechnet werden. Da es sich dabei um eine sogenannte abhängige oder Kriteriumsvariable (*tatsächliches Datenschutz-Verhalten*) handelt, die von vier unabhängigen oder Prädiktorvariablen (*Alter*, *Geschlecht*, *subjektives Wissen* und *objektives Wissen*) vorhergesagt werden soll, eignet sich hierfür die sogenannte multiple Regressionsanalyse (Bortz, 2005). Die Voraussetzungen, die ein Datensatz erfüllen muss, bevor eine solche Analyse durchgeführt werden kann, sind:

- Lineare Beziehung zwischen den Variablen
- keine Ausreißer
- Unabhängigkeit der Residuen
- Keine Multikollinearität
- Homoskedastizität (Gleichheit der Varianzen) der Residuen
- Normalverteilung der Residuen

Um die lineare Beziehung zwischen den kontinuierlichen Variablen zu überprüfen, werden mit Hilfe des Statistikprogrammes SPSS jeweils partielle Regressionsdiagramme (siehe Anhang E.1) für den Zusammenhang jeder einzelnen Prädiktorvariablen mit der Kriteriumsvariable generiert. Ein partielles Regressionsdiagramm stellt auf der X-Achse das sich ergebende Residuum dar, wenn eine Prädiktorvariable, z. B. *Alter* in Bezug auf alle anderen Prädiktorvariablen einer Regression unterzogen wird. Die Residuen stellen die Abweichungen der empirischen Werte von den vorhergesagten Werten dar (Bortz, 2005). Auf der Y-Achse ist das entstehende Residuum dargestellt, wenn die Kriteriumsvariable auf alle Prädiktorvariablen außer dieser einzelnen (*Alter)* regressiert wird. Das bedeutet, der durch alle anderen Prädiktorvariablen nicht erklärte Teil des *Datenschutz-Scores* wird gegen den von den anderen Prädiktorvariablen unabhängigen Teil von *Alter* abgetragen. Zeigen sich hier Anzeichen einer linearen Beziehung, wird davon ausgegangen, dass Linearität vorliegt. Die Streudiagramme werden deshalb augenscheinlich nach einem linearen Zusammenhang überprüft. Wenn auch schwach zeigen die Variablen hier Hinweise auf lineare Beziehungen. Die Abbildungen der Streudiagramme und die SPSS Ausgaben der folgenden Berechnungen sind in Anhang E dieser Arbeit zu finden.

Im nächsten Schritt wurden die Datensätze augenscheinlich nach Ausreißern überprüft, die allerdings im Rahmen der vorangegangenen Analysen schon aufgefallen wären. Diese Voraussetzung gilt somit auch als erfüllt. Um die Unabhängigkeit der Residuen zu überprüfen, zieht man die sogenannte Durbin-Watson-Statistik zu Rate, die SPSS ausgibt (siehe Anhang E.2). Liegt diese wie in diesem Fall mit 2,161 zwischen 1.5 und 2.5, ist nicht von einer Autokorrelation der Residuen auszugehen (Rudolf & Müller, 2011). Multikollinearität, ist bei wechselseitiger, linearer Abhängigkeit von zwei oder mehr der Prädiktoren gegeben (Bortz, 2005). Dies würde klare Vorhersagen verhindern. Multikollinearität lässt sich mit Hilfe des VIF-Wertes (VIF=Varianzinflationsfaktor Rudolf & Müller, 2011) im SPSS Output (siehe Anhang E.3) überprüfen. In diesem Fall liegen die sich ergebenden Werte zwischen 1,003 (Alter) und 1,416 (objektives Wissen) und damit weit unter der Toleranz von 10 (Myers, 1990). Es liegt demnach keine Multikollinearität vor. Die Gleichheit der Varianzen der Residuen oder auch Homoskedastizität wird mittels eines Streudiagrammes zwischen den unstandardisierten, vorhergesagten Werten und den Residuen (siehe Anhang E.4) untersucht, welches in SPSS ausgegeben werden kann. Dabei sollte sich die ausgegebene Punktewolke gleichmäßig zur horizontalen Achse verteilen. Auch diese Voraussetzung kann als erfüllt angesehen werden. Um die letzte Voraussetzung der Normalverteilung der Residuen zu überprüfen, gibt es mehrere Möglichkeiten. In diesem Falle wird der sogenannte P-P-Plot in der Ausgabe von SPSS (siehe Anhang E.5) gewählt. In diesem ist die erwartete kumulierte Wahrscheinlichkeit gegen die beobachtete kumulierte Wahrscheinlichkeit abgetragen. Je weiter die sich ergebenden Punkte von der Diagonalen entfernt liegen, desto weniger kann man von normalverteilten Residuen ausgehen. In diesem Falle sind einige Abweichungen zu erkennen. Da es sich bei der multiplen Regression allerdings um ein eher robustes Verfahren bezüglich Verletzungen der Normalverteilungsannahmen handelt, wird auch diese Voraussetzung als ausreichend erfüllt angesehen.

Die eigentliche Regressionsrechnung, die in SPSS zunächst durchgeführt werden muss, um anhand der Ausgabe die Voraussetzungen überprüfen zu können, kann demnach interpretiert werden. In diesem Fall ergibt sich ein Modell (siehe Anhang E.6), welches mit einem *p*-Wert von .107 gerade eben nicht mehr (auf dem 10%-Niveau) signifikant wird. Aus diesem Grund wurde sich für eine weitere Analyse im Sinne der sogenannten schrittweisen Regression entschieden. Hierbei werden die Prädiktoren nacheinander in das Regressionsmodell einbezogen, beginnend mit der Variable mit der höchsten Validität (Bortz, 2005). Weitere Variablen werden nur dann in das Modell einbezogen, wenn sie das bereits existierende Vorhersagepotential erhöhen (Bortz, 2005). Es ergibt sich dabei ein Modell mit einer Signifikanz von $p=.013$ und einer erklärten Varianz von $R^2=.090$ (siehe Anhang E.7). Generell kann der multiple

Determinationskoeffizient R^2, der eine Aussage bezüglich des Verhältnisses der Varianz der vorhergesagten Werte zu der Varianz der beobachteten Werte macht, Werte zwischen 0 und 1 annehmen (Eid et al., 2010). Eine erklärte Varianz von .090 stellt somit einen sehr geringen Anteil erklärter Varianz dar. Als einziger signifikanter Prädiktor (p=.013) mit einem Regressionskoeffizienten B von -.023 ergibt sich die Variable *Alter*. Diese sagt demnach das Kriterium *tatsächliches Datenschutz-Verhalten* statistisch signifikant voraus, F(4,63)=1,990, p=.013. Inhaltlich weist der negative Regressionskoeffizient auf einen negativen Zusammenhang hin, was bedeutet, je älter die Probanden, desto weniger ausgeprägt war deren Datenschutz-Verhalten.

Das zweite zu überprüfende Modell besteht aus den beiden Prädiktoren *wahrgenommenes Risiko im Internet Daten anzugeben, ohne die Datenschutzerklärungen angeschaut zu haben* und dem entsprechenden *erwarteten Nutzen*. Beide sollen zum einen eine Vorhersage bezüglich der angegebenen *Wahrscheinlichkeit dafür machen im Internet Daten anzugeben, ohne die Datenschutzerklärungen angeschaut* zu haben. Da die angegebene Wahrscheinlichkeit ein risikoreiches Verhalten zu zeigen als guter Prädiktor, wenn nicht sogar als Entsprechung für tatsächliches Verhalten gilt (z. B. Ajzen, 1991; Fishbein & Ajzen, 1975; Pfeiffer et al., 2013), werden alle drei Faktoren im zu prüfenden Modell als Prädiktoren für das *tatsächliche Verhalten im Internet Daten anzugeben, ohne die Datenschutzerklärungen angeschaut zu haben,* verwendet. Diese Kriteriumsvariable kam zustande, indem für jeden Probanden im Rahmen der Blickbewegungsanalyse untersucht wurde, ob mindestens eine Fixation auf einer entsprechenden AOI stattgefunden hat. Die beiden möglichen Ausprägungen, ob der Hinweis überprüft wurde oder eben nicht, führt dazu, dass es sich um eine dichotome Variable handelt. Um ein solches Modell zu überprüfen, wird im Gegensatz zum vorangegangenen Modell keine multiple Regression, sondern eine sogenannte multiple logistische Regression verwendet (Eid et al., 2010). Der Einfluss von wahrgenommenem Risiko und erwartetem Nutzen auf die Wahrscheinlichkeit und wiederum der Einfluss dieser drei Variablen auf das tatsächliche Verhalten kann in diesem Fall allerdings nicht gleichzeitig in einem Modell überprüft werden. Das liegt an der für die Berechnung eines sogenannten Strukturgleichungsmodelles zu kleinen Stichprobe. Die für ein solches Modell mit ausschließlich sogenannten manifesten Variablen gebräuchliche Methode der Pfadanalyse eignet sich darüber hinaus nicht in den Fällen, in denen die abhängige Variable nicht metrisch skaliert ist (Weiber & Mühlhaus, 2014). Ein Merkmal gilt als manifestes im Gegensatz zu einem latenten Merkmal, wenn die jeweilige Ausprägung direkt erkennbar, bzw. eindeutig ist (Döring & Bortz, 2016). Es wurden zur Überprüfung deshalb zwei Regressionen gerechnet. Zur Vorhersage der angegebenen Wahrscheinlichkeit eine multiple Regression und zur Vorhersage der dichotomen Variablen des tatsächlichen Verhaltens eine multiple logistische Regression. Im Vorfeld der multiplen Regressionsrechnung wurden erneut die oben beschriebenen Voraussetzungen geprüft (siehe Anhang F.1-F.5). Bei Betrachtung des P-P-Plots erscheint eine Normalverteilung der Residuen zwar noch unwahrscheinlicher als bei der vorangegangenen Analyse, alle anderen Voraussetzungen werden aber als erfüllt angesehen.
Die eigentliche Analyse kommt mit einem p-Wert von .016 zu einem signifikanten Ergebnis (siehe Anhang F.6). Es ergibt sich eine erklärte Varianz von R^2=.124, was immer noch einem eher kleinen Effekt entspricht. Es bedeutet, dass 12,4% der Varianz in den Daten bezüglich der Variable *Wahrscheinlichkeit im Internet Daten anzugeben, ohne die Datenschutzerklärungen angeschaut zu haben* durch dieses Modell erklärt werden. Als einziger signifikanter Prädiktor zeigt sich dabei allerdings das *wahrgenommene Risiko im Internet Daten anzugeben, ohne die Datenschutzerklärungen angeschaut zu haben* mit einem Regressionskoeffizienten B von -.445. Es lässt sich also sagen, dass der Prädiktor *wahrgenommenes Risiko im Internet Daten anzugeben, ohne die Datenschutzerklärungen angeschaut zu*

haben das Kriterium *Wahrscheinlichkeit im Internet Daten anzugeben, ohne die Datenschutzerklärungen angeschaut zu haben* statistisch signifikant vorhersagt, $F(2,62)=4{,}395$, $p=.016$.
Die im nächsten Schritt zu verwendende multiple logistische Regression unterliegt erheblich weniger Voraussetzungen an das zu Verfügung stehende Datenmaterial (Backhaus, Erichson, Plinke & Weiber, 2016). So muss die abhängige (oder Kriteriums-) Variable kategorial vorliegen und es wird eine größere Stichprobe benötigt als bei der linearen Regression. Pro unabhängiger Variable sollten mindestens 10 Fälle vorhanden sein und diese untereinander möglichst frei von Multikollinearität sein (Backhaus et al., 2016). Die Erfüllung dieser Voraussetzung wurde im Rahmen der vorherigen Analyse ja bereits untersucht. Die Voraussetzungen werden somit als erfüllt angesehen. Die eigentliche Analyse wird wieder mit der Statistiksoftware SPSS durchgeführt. Mit p-Werten von $p=.306$ (*wahrgenommenes Risiko…*), $p=.437$ (*erwarteter Nutzen…*) und $p=.449$ (*angegebene Wahrscheinlichkeit…*) wurde allerdings keiner der Prädiktoren signifikant (siehe Anhang F.7). Auch der Ausschluss der Variable *Wahrscheinlichkeit im Internet Daten anzugeben, ohne die Datenschutzerklärungen angeschaut zu haben* führte zu keiner Verbesserung des Modells. Um abschließend eine letzte Prüfung eines Zusammenhanges zwischen der *angegebenen Wahrscheinlichkeit…* und dem *tatsächlichen Verhalten* durchzuführen, wird eine punktbiserialen Korrelation mit SPSS berechnet. Diese ist geeignet, um den Zusammenhang einer Intervallskala mit einem dichotomen Merkmal zu überprüfen (Bortz, 2005). Mit $p=.472$ kommt auch diese zu dem Ergebnis, dass kein Zusammenhang zwischen der *angegebenen Wahrscheinlichkeit im Internet Daten anzugeben, ohne die Datenschutzerklärungen angeschaut zu haben* und dem *tatsächlichen Verhalten im Internet Daten anzugeben, ohne die Datenschutzerklärungen angeschaut zu haben* besteht (siehe Anhang F.8).

5.5 Validierte Modelle des Datenschutzverhaltens beim Onlineshopping

Auf Basis der durchgeführten multiplen Regression wurden die Variablen *Geschlecht*, *objektives Wissen* und *subjektives Wissen* aus dem in Kapitel 4.1 aufgestellten und in Kapitel 5.1 angepassten Modell ausgeschlossen. Der Teil des Modells, dessen Nachweis im Rahmen der vorangegangenen Analyse gelang, besteht nun aus dem Prädiktor *Alter*, der eine Vorhersage bezüglich des Datenschutz-Verhaltens beim Onlineshopping macht. Das sich ergebende Modell ist in Abbildung 20 dargestellt.

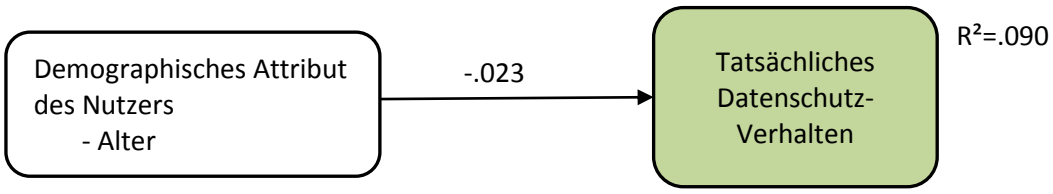


Abbildung 20. Validiertes Modell zur Vorhersage von Datenschutz-Verhalten beim Onlineshopping.

Das zweite Modell, welches die Vorhersage einer ganz konkreten risikoreichen Handlung zum Ziel hatte, wurde in zwei Schritten überprüft. Eine multiple lineare Regression kam zu dem Ergebnis, dass ein Einfluss des wahrgenommenen Risikos auf die angegebene Wahrscheinlichkeit dafür dieses Verhalten zu zeigen, besteht. Ein Zusammenhang zwischen den Prädiktoren und dem Kriterium des tatsächlichen Verhaltens konnte nicht nachgewiesen werden. Abbildung 21 stellt den gefundenen Zusammenhang im Rahmen des zweiten Modells dar.

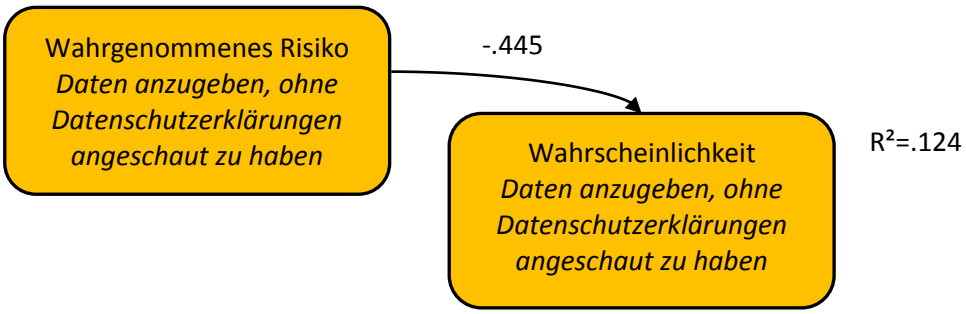


Abbildung 21. Nachgewiesener Zusammenhang bezüglich des Modells zur Vorhersage des tatsächlichen Verhaltens *im Internet Daten anzugeben, ohne vorher die Datenschutzerklärungen angeschaut zu haben*.

Die beiden validierten Modelle geben somit Antwort auf *Forschungsfrage 2: Welche personenbezogenen Faktoren haben einen Einfluss auf das tatsächliche Datenschutz-Verhalten beim Onlineshopping*? und *Forschungsfrage 3: Inwieweit lässt sich das tatsächliche Datenschutz-Verhalten beim Onlineshopping mit Hilfe der gefundenen Einflussfaktoren vorhersagen?*
Die im Rahmen dieser Arbeit dargestellten Erkenntnisse und das gesamte Vorgehen werden im folgenden Kapitel diskutiert.

6 Diskussion

Der Einkauf unterschiedlicher Waren im Internet ist eine weit verbreitete Aktivität, die unterschiedlichsten Risiken unterliegt (vergleiche Kapitel 2.2). Trotzdem steigt die Nutzung immer weiter an (Boos, 2015). Die persönlichen Daten im Rahmen dieser Aktivität zu schützen wird in der Presse als das „neue Videorecorder-Programmieren“ betitelt (Business Insider Inc, 2010). Gemeint ist, dass sich Onlineshoppingnutzer mit dieser Aufgabe häufig überfordert fühlen (Wambach, 2017) und nur wenige sie beherrschen. Befragt man Nutzer danach, ob sie Ihre persönlichen Daten schützen, so werden sie das häufig bejahen, obwohl dies nicht der Realität entspricht (siehe Privacy-Paradoxon, Kapitel 1.1 und 2.4.2). Eine Vorhersage dieses Verhaltens auf Basis der erfragten Intention scheint demnach nicht zielführend. In der Erfassung von tatsächlichem Datenschutz-Verhalten beim Onlineshopping als Basis einer Vorhersage, wurde im Rahmen dieser Arbeit eine Forschungslücke gesehen. Als ein Ziel (*Forschungsfrage 1: Wie lässt sich tatsächliches Datenschutz-Verhalten beim Onlineshopping empirisch erfassen?*) ergab sich deshalb, eine Möglichkeit zu finden, das tatsächliche Verhalten von Personen zum Schutz ihrer persönlichen Daten im Rahmen des Onlineshoppings empirisch zu erfassen. Hierfür wurde im ersten Schritt eine Operationalisierung von tatsächlichem Datenschutz-Verhalten beim Onlineshopping erarbeitet (*Forschungsfrage 1a: Wie kann tatsächliches Datenschutz-Verhalten beim Onlineshopping operationalisiert werden?*; Kapitel 3.1). Basis der Operationalisierung ist die Definition dieses Konstruktes, welche im Rahmen dieser Arbeit erarbeitet wurde (Kapitel 2.1.1-2.1.4). Im Anschluss wurde eine Liste von potentiellen Hinweisen erstellt, die Nutzer beim Besuch eines ihnen unbekannten Webshops dazu verwenden können, dessen Vertrauenswürdigkeit einzuschätzen (Kapitel 3.1.1). Da Fixationen der Nutzer auf diesen Hinweisen als Überprüfung des entsprechenden Hinweises gewertet werden sollten, war es notwendig zuvor die hier verwendete Definition für Fixationen festzulegen (Kapitel 3.1.2). Um festzustellen, ob sich die Wichtigkeit der Überprüfung der verschiedenen Hinweise insgesamt und bezüglich der notwendigen Intensität unterscheidet, wurde dann eine Gewichtungsstudie im Rahmen einer Expertenbefragung durchgeführt (Kapitel 3.2.1). Diese führte zu acht Hinweisen, die von den Experten als am wichtigsten eingeschätzt wurden (Kapitel 3.2.2). Darüber hinaus ergab sie deren eingeschätzte Wichtigkeit dafür, mittels eines kurzen Blickes zu überprüfen, ob der jeweilige Hinweis vorhanden ist und die Wichtigkeit dafür, diesen Hinweis darüber hinaus zu betrachten. Statistisch konnten keine Unterschiede zwischen diesen Wichtigkeiten und auch zwischen den Hinweisen selbst nachgewiesen werden. Zur Quantifizierung des Datenschutz-Verhaltens (*Forschungsfrage 1b: Wie kann erhobenes Verhalten für weitere Analysen quantifiziert werden?*) wird deshalb die Summe der Hinweise aus diesen acht wichtigsten Hinweisen verwendet, die von einer am Versuch teilnehmenden Person fixiert wurden. Im nächsten Schritt wurden Anforderungen an eine entsprechende Erhebung gesammelt, die sich unter anderem aus diversen Einschränkungen ergaben, denen bisherige Studien in diesem Bereich unterliegen (*Forschungsfrage 1c: Welche Anforderungen bestehen an eine solche empirische Erhebung?;* Kapitel 3.3). Die Erarbeitung dieser Grundlagen zur empirischen Erfassung des Datenschutz-Verhaltens beim Onlineshopping stellte die Basis der folgenden Explorationsstudie dar, die zur Beantwortung der zweiten Forschungsfrage (*Forschungsfrage 2: Welche personenbezogenen Faktoren haben einen Einfluss auf das tatsächliche Datenschutz-Verhalten beim Onlineshopping*?), bezüglich potentieller personenbezogener Einflussfaktoren durchgeführt wurde (Kapitel 4).

Dabei wurde ein sogenannter Top-Down Ansatz verwendet, bei dem ausgehend von einem Modell die Blickbewegung zur Überprüfung aller oder nur einzelner Aspekte des Modells verwendet wird (Goldberg et al., 2002). Hierfür wurden die in Kapitel 2.4.1 dargestellten Erkenntnisse bezüglich Einflussfaktoren

auf Risikoverhalten zu einem Arbeitsmodell zusammengefasst, aus dem sich Hypothesen ableiten ließen (Kapitel 4.1). Mittels der in Kapitel 4.2 beschriebenen Explorationsstudie konnten die Variablen des Arbeitsmodells erfasst werden. Die Ergebnisse dieser Studie sind in Kapitel 4.3 dargestellt. Bezüglich der potentiellen Prädiktoren auf das erfasste tatsächliche Verhalten ergaben sich zwar keine nachweislichen Zusammenhänge, es wurden aber aussichtsreiche Variablen ermittelt (Kapitel 4.4). Das Vorgehen und die Ergebnisse der Explorationsstudie wurden anschließend diskutiert (Kapitel 4.5). Die gewonnenen Erkenntnisse wurden im nächsten Schritt genutzt, um das in Kapitel 4.1 erarbeite Arbeitsmodell so anzupassen, dass dieses auch unter Verwendung einer sich aus zeitlichen und monetären Ressourcen begründenden kleineren Stichprobe überprüfbar bleibt (Kapitel 5.1). Dafür wurde auf die Erkenntnisse bezüglich potentieller Prädiktoren, die im Rahmen der Explorationsstudie gemacht wurden, zurückgegriffen. Um die Tauglichkeit dieser potentiellen Prädiktoren auf das tatsächliche Datenschutz-Verhalten beim Onlineshopping überprüfen und eine Aussage bezüglich der Vorhersage dessen machen zu können, wurde im Anschluss daran eine Validierungsstudie durchgeführt (Kapitel 5.2). Diese glich, bis auf kleinere Anpassungen, prinzipiell in Aufbau und Vorgehen der Explorationsstudie. Die Ergebnisse der Validierungsstudie sind in Kapitel 5.3 dargestellt. Hier stellte sich z. B. die Frage, inwieweit die Hinweise auf Webseiten bezüglich des Umgangs mit personenbezogenen Daten tatsächlich Beachtung bei den Nutzern finden (Ahrholdt, 2010; Wang et al., 2004). Diesbezüglich zeigte sich, dass alle Hinweise insgesamt wenig zur Orientierung verwendet wurden. Am häufigsten (von 23 von den insgesamt 73 Teilnehmern) wurde der Hinweis *Shopname (URL)* fixiert, gefolgt von *Informationen zu Datenschutz* (19 Teilnehmer) und den *Gütesiegeln* (16 Teilnehmer). Bei Downs et al. (2006) lag der Anteil der Probanden, die Unregelmäßigkeiten in der URL bemerkten bei 55%. Hierbei sei allerdings bemerkt, dass es sich dabei um die Bearbeitung von Emails im Kontext von Phishing handelte. Es wird vermutet, dass in die Informationsfülle, die sich dem Nutzer darstellt, geringer ist, als dies im Kontext des Onlineshoppings häufig der Fall ist. Die Sichtbarkeit von Auffälligkeiten wäre damit erhöht. Im Rahmen des Datenschutz-Scores zur Quantifizierung des tatsächlichen Verhaltens, der sich aus der Summe der betrachteten wichtigsten Hinweise errechnete, betrug der höchste erhaltene Wert nur vier, bei acht möglichen Punkten. Diese Ergebnisse bestätigen die Aussage von Whalen und Inkpen (2005), dass Sicherheitshinweise insgesamt nur wenig beachtet werden. Laut Wu et al. (2006) kann das darin begründet liegen, dass die Nutzer vordergründig mit anderen Aufgaben wie dem Lesen von Emails, der Bearbeitung eines Dokumentes oder eben, wie in diesem Fall, dem Kauf eines Produktes beschäftigt sind und der Schutz der persönlichen Daten eine untergeordnete Rolle einnimmt. Es sei an dieser Stelle erwähnt, dass die Experten jeweils nur die fünf wichtigsten Hinweise nannten. Möglicherweise ist eine Überprüfung von nur vier Hinweisen ausreichend, um eine Vorstellung bezüglich der Vertrauenswürdigkeit zu bekommen.

Die Erkenntnisse bezüglich der Vorhersage des tatsächlichen Datenschutz-Verhaltens sind in Kapitel 5.4 zusammengefasst. Diesbezüglich zeigte sich, dass der Einfluss des Alters als einziger dieser personenbezogenen Faktoren nachgewiesen werden konnte, was der Beantwortung von Forschungsfrage 2 entspricht. Die sich ergebende negative Gewichtung gibt dabei einen Hinweis darauf, dass je älter der jeweilige Nutzer, bzw. die Nutzerin ist, desto weniger ausgeprägt ist das entsprechende Datenschutzverhalten. Entgegen der Ergebnisse von Downs et al. (2006) gehen die jüngeren Probanden in dieser Studie somit ein geringeres Risiko ein. Dies geht einher mit den Ergebnissen von Chadwick-Dias et al. (2003), die besagen, dass ältere Nutzer mehr Probleme bei der Nutzung des Internets haben als jüngere, was sie zu einer sehr wichtigen Nutzer-Gruppe macht. Urbany, Dickson und Wilkie (1989) argumentieren diesbezüglich, dass Nutzer im Zuge des Älterwerdens Erfahrungen und Wissen anhäufen. Dagegen erwähnen Anderson und Agarwal (2010), dass private Nutzer selbst die Initiative ergreifen und sich in Bezug auf Maßnahmen zu Sicherheit im Internet selbst schulen müssten. Dabei lernen sie laut

van Deursen und van Dijk (2010) häufig durch Ausprobieren, was dazu führen kann, dass, solange nichts passiert, sie die gleichen Fehler immer wieder machen. Die beiden Autoren konnten in ihrer Arbeit einen Zusammenhang zwischen dem Alter und den Internetfähigkeiten nachweisen. Es ist somit davon auszugehen, dass ältere Probanden demnach möglicherweise nicht bewusst ein Risikoverhalten zeigen, sondern umgekehrt ihr Schutzverhalten weniger ausgeprägt ist. Dies ist eine Tatsache, die insgesamt im Rahmen dieser Arbeit erwähnt werden muss. Während, wie in Kapitel 2.4.3.1 dargestellt, häufig bei Untersuchungen im Rahmen der Forschung zu Verhalten bezüglich des Datenschutzes (privacy-Forschung) die Art und/oder Anzahl der preisgegebenen Daten als Messgröße verwendet werden (z. B. Amichai-Hamburger & Vinitzky, 2010; Norberg et al., 2007), wurde im Rahmen dieser Arbeit vielmehr das davor stehende Verhalten zum Schutz dieser preiszugebenden Daten erfasst. Häufig wird in diesen Studien die Definition von Westin (1967) für *privacy* verwendet. *Privacy* ist dort beschrieben, als "ability of individuals to determine the nature and extent of information about them which is being communicated to others" (Westin 1967, in Campbell, 1997, S. 45). Die Messgröße der preisgegebenen Daten stellt damit vielmehr das Ergebnis dieser Fähigkeit (*ability*) dar. Unterschiede bezüglich der Ergebnisse und Einflussfaktoren zwischen dieser und anderen Studien können sich demnach auch daher ergeben.

Neben dem Einfluss der personenbezogenen Daten auf das globale Datenschutz-Verhalten sollte eine Vorhersage bezüglich einer spezifischen Handlung gemacht werden. Hierfür wurde *im Internet Daten anzugeben, ohne die Datenschutzerklärungen angeschaut zu haben* gewählt. Dies entsprach dem von den Experten am häufigsten zu den wichtigsten Hinweisen gezählten Hinweis. Im Rahmen dieser Untersuchung konnte der in der Literatur bereits häufig beschriebene Zusammenhang zwischen dem jeweiligen wahrgenommenen Risiko und der im Fragebogen angegebenen Wahrscheinlichkeit dafür, diese Handlung zu vollziehen (z. B. Figner & Weber, 2011; Hanoch et al., 2006), repliziert werden. Der erwartete Nutzen stellte in diesem Fall keinen signifikanten Prädiktor dar. Eine Vorhersage des tatsächlichen Verhaltens, also ob ein Proband auf einen solchen Hinweis geschaut hatte oder nicht, gelang mit Hilfe des wahrgenommenen Risikos, des erwarteten Nutzens und der Wahrscheinlichkeit für das Verhalten nicht. Es konnte kein Zusammenhang zwischen der angegebenen Wahrscheinlichkeit und dem tatsächlichen Verhalten nachgewiesen werden. Diese Tatsache entspricht dem Privacy Paradoxon und wird von Norberg et al. (2007) damit begründet, dass in beiden Fällen unterschiedliche Bezugsrahmen vorliegen. Fragt man eine Person direkt nach ihrer Intention, bzw. der Wahrscheinlichkeit Daten preiszugeben, dann beeinflusst das wahrgenommene Risiko die Antwort. Diese Erklärung kann auch mit Hilfe des hier nachgewiesenen Zusammenhanges zwischen dem wahrgenommenen Risiko und der angegebenen Intention bekräftigt werden. In der tatsächlichen Situation aber soll das in diesem Rahmen nicht erhobene Vertrauen eine größere Rolle spielen (Norberg et al., 2007).

Im vorliegenden Fall führt die signifikante Vorhersage des Datenschutz-Verhaltens mittels der Variable Alter zu einer, wenn auch nur geringen, Varianzaufklärung (*Forschungsfrage 3: Inwieweit lässt sich das tatsächliche Datenschutz-Verhalten beim Onlineshopping mit Hilfe der gefundenen Einflussfaktoren vorhersagen?*). Daraus lässt sich schließen, dass vor allem andere Faktoren als die hier untersuchten personenbezogenen Daten Einfluss auf dieses Verhalten haben.

6.1 Diskussion bezüglich der verwendeten Methoden

An dieser Stelle werden die im Rahmen der Studien verwendeten Methoden diskutiert. Diese unterteilen sich in die Expertenbefragung via Online-Fragebogen (Kapitel 6.1.1), in der Explorations- und der

Validierungsstudie verwendete Fragebögen (Kapitel 6.1.2), die gestellte Online-Aufgabe (Kapitel 6.1.3) und die Blickbewegungsanalyse (Kapitel 6.1.4)

6.1.1 Expertenbefragung via Online-Fragebogen

Die Methode der Expertenbefragung, die im Rahmen dieser Arbeit mit Hilfe eines Online-Fragebogens durchgeführt wurde, wurde in Teilen bereits in Kapitel 3.2.3 diskutiert. Dabei beziehen sich die dort genannten Vorteile wie die ressourcenschonende Durchführung (Hewson et al., 1996), die freie Auswahl des Bearbeitungszeitpunktes (Huber, 2005) und die gegebene Erreichbarkeit der Zielgruppe (Döring & Bortz, 2016; Gosling et al., 2004) auf die Methode des Online-Fragebogens. Dies gilt auch für den dort diskutierten, eventuell nachteiligen Einsatz von zwei unterschiedlichen Reglern, die Möglichkeit, dass die Befragung eher abgebrochen wird (Huber, 2005), sowie die Einschränkung, dass eventuell nicht alles von allen Teilnehmern und Teilnehmerinnen auf die gleiche Weise verstanden wurde (Kraut et al., 2004).
In Bezug auf die Expertenbefragung als Methode lässt sich sagen, dass diese von Döring und Bortz (2016) als Lösung im Falle einer Gewichtung, bzw. normativen Indexbildung, empfohlen wird. Auch Ahrholdt (2010) verwendete im Rahmen seiner Arbeit ein Expertenrating, um die Wichtigkeit verschiedener Hinweise einschätzen zu lassen. Das Kriterium dafür war in seiner Arbeit allerdings die Relevanz der Signale in Bezug auf den wirtschaftlichen Erfolg eines Anbieters.
Als Schwierigkeit dieser Methode erwähnen Döring und Bortz (2016) die beschränkte Erreichbarkeit dieser Zielgruppe, die in den meisten Fällen zu einer kleinen Anzahl tatsächlicher Teilnehmer führt. Auch im Rahmen dieser Arbeit konnten nur 10 Experten für die Teilnahme gewonnen werden, wobei nur die Daten von neun Teilnehmern auswertbar waren. An dieser Stelle sei erwähnt, dass Einiges versucht wurde, die Anzahl zu erhöhen, wie z. B. die Kontaktierung verschiedener öffentlicher Institutionen, die sich mit Datenschutz beschäftigen oder die Nutzung von Emailverteilern thematisch entsprechender universitärer Projekte. So wurde auch die Erreichbarkeit des Online-Fragebogens zusätzlich verlängert. Obwohl die Einschätzungen weiterer Experten an dieser Stelle wünschenswert gewesen wären, kann aber, wie bereits in der Diskussion der Gewichtungsstudie erwähnt, die sich ergebende Anzahl von Teilnehmern als ausreichend angesehen werden.
Interessant ist dabei die gewollte Zusammensetzung der Experten-Stichprobe aus unterschiedlichen wissenschaftlichen Hintergründen. Wie von Bartsch et al. (2014) erwähnt, ist die Einbeziehung unterschiedlicher Fachdisziplinen diesbezüglich in der Vielfalt der vorhandenen Risiken begründet. Dies zeigte sich auch in den unterschiedlichen Beurteilungen der Wichtigkeit der Hinweise, die sich teilweise auf die unterschiedlichen wissenschaftlichen Hintergründe beziehen lassen. Somit sollte die erwähnte Vielfalt der Risiken in die Gewichtung der zur Operationalisierung verwendeten Hinweise einfließen.

6.1.2 Fragebögen der Explorations- und Validierungsstudie

Bezüglich der verwendeten Fragebögen lässt sich sagen, dass diese generell ein gängiges Instrument zur Erfassung personenbezogener Daten in der psychologischen Forschung sind (Döring & Bortz, 2016). Die Operationalisierung der Variablen und Ausformulierung der einzelnen Items orientiert sich im Rahmen dieser Arbeit an Literatur desselben Themenbereichs. So entsprachen die Items zur Beschreibung der Personen und deren Antwortformate denen der Grundlagenstudie des SINUS-Instituts Heidelberg im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI) (SINUS-Institut Heidelberg, 2012). In dieser wurden Internetnutzer mittels ihrer demographischen Daten und

darüberhinausgehenden Angaben unterschiedlichen Nutzertypen zugeordnet. Aufgrund fehlender Trennschärfe konnten diese Typen aber nicht im Rahmen einer Vorhersage in dieser Arbeit verwendet werden.
Das Gerüst der Befragung zu wahrgenommenen Risiko, erwarteten Nutzen und der entsprechenden Wahrscheinlichkeit für ein Verhalten, stellt die in Kapitel 2.4.1 vorgestellte Domain-Specific Risk-Taking Scale (Weber et al., 2002) dar. Hier wurden die verwendeten in der Realität stattfindenden Risikohandlungen, wie z. B. *sich beim Autofahren nicht anschnallen* durch Situationen, die im Internet stattfinden, ersetzt. Zur Einleitung in die jeweilige Fragestellung wurden die originalen Aufgabenbeschreibungen der deutschen Version verwendet (*DOSPERT.org;* Johnson et al., 2004). Statt deren *bereichspezifischen Risikoskala* mit Stufen von 1 bis 7, wurde in diesem Fall eine Visuelle Analog Skala verwendet. Da in keiner der durchgeführten Prä-Studien Probleme bezüglich dieser Skala erwähnt wurden, wird hier davon ausgegangen, dass dies zu keinen Verzerrungen führte. Die letztlich zur Vorhersage des tatsächlichen Datenschutz-Verhaltens verwendete Handlung *im Internet Daten anzugeben, ohne die Datenschutzerklärungen angeschaut zu haben* gilt als relevant, da der Hinweis *Informationen zu Datenschutz/Datensicherheit* am häufigsten von den Experten im Rahmen der Gewichtungsstudie als einer der wichtigsten Hinweise genannt wurde.
Wie in Kapitel 2.4.1 dargestellt, existieren einige Forschungsergebnisse zu unterschiedlichem Verhalten oder Einschätzungen zwischen Experten und nicht-Experten. Die verwendeten Methoden, um diese beiden Gruppen zu unterscheiden, sind vielfältig und häufig strittig. Besonders die häufig eingesetzte Methode der Selbsteinschätzung stellt dabei keine akkurate Messmethode dar (van Deursen & van Dijk, 2010). Auf Selbstauskünfte zur Einschätzung der Fähigkeiten der Probanden sollte deshalb verzichtet werden (Hargittai, 2005). Da in der Literatur zu diesem Zeitpunkt kein geeigneter Fragebogen zu finden war, dessen Fokus auf der Abfrage des Wissens über Datenschutz lag, wurde in interdisziplinärer Zusammenarbeit zwischen Psychologen und Informatikern ein entsprechender Fragebogen erarbeitet. Dieser wurde im Rahmen von studentischen Arbeiten (Bäuerlein et al., 2013; Debel et al., 2013; Goldstein et al., 2013) bezüglich Größen, wie Itemschwierigkeiten, Trennschärfe, Validität und Reliabilität untersucht und angepasst. Im Rahmen dieser Arbeit wurden Auszüge aus diesem Fragebogen zur Erfassung des subjektiven oder wahrgenommenen und des objektiven oder tatsächlichen Wissens verwendet. Die Tatsache, dass die erhaltenen Werte dabei der Form von Normalverteilungen entsprechen, spricht dafür, dass mit Hilfe des Fragebogens eine differenzierte Einteilung der Teilnehmer vorgenommen werden konnte.

6.1.3 Online-Aufgabe und Interview

Die empirische Erfassung des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping verwendete eine Online-Aufgabe, die zuerst dazu aufforderte sich ein Produkt auszusuchen, welches man kaufen möchte, und dieses dann im nächsten Schritt bei einem unbekannten Webshop so günstig wie möglich zu kaufen. Damit sollte sie möglichst alle drei von Holmqvist et al. (2011) aufgestellten Kriterien für eine gute Aufgabe erfüllen. So ist sie neutral gegenüber den experimentellen Bedingungen, ist so einnehmend, dass sie die Probanden von der Blickbewegung ablenkt und beinhaltet eine Art Cover-Story, die den Fokus eher auf den Einkauf im Internet als auf Datensicherheit lenkt. Während sich die Teilnehmer also in erster Linie mit der Bearbeitung der Aufgabe, nämlich dem Onlineeinkauf beschäftigen, wird das Verhalten zum Schutz der personenbezogenen Daten beobachtet. Jeder der 91 Probanden bekam unbegrenzt Zeit, um diese Aufgaben zu bearbeiten. So dauerte der Versuch jedes Mal zwischen 1 und 1,5 Stunden. Hierfür wurde jedem Teilnehmer eine Aufwandsentschädigung von 10 €

gezahlt. Wie bereits erwähnt, führt eine solch umfangreiche Untersuchung somit zu nicht unerheblichen Kosten in Bezug auf Geld und Zeit (van Deursen & van Dijk, 2010).

Kombiniert wurde die Aufgabe mit den beiden anschließenden Interviewfragen danach, ob sich der Teilnehmer, bzw. die Teilnehmerin anders verhalten hat, als sie/er sonst beim Onlineshopping agiert und woran sie, bzw. er sich bei der Auswahl eines vertrauenswürdigen Anbieters orientiert habe. Die zweite Frage wurde im Rahmen dieser Arbeit nicht explizit ausgewertet. Die Antworten weisen aber in den seltensten Fällen auf die Orientierung anhand datenschutzorientierter Hinweise hin. Vielmehr wurden hier Argumente wie die Bekanntheit des verwendeten Webshops oder Preis und Qualität der Produkte genannt. Die erste Interviewfrage dagegen führte im Rahmen der Explorationsstudie zum Ausschluss einiger Teilnehmer, die antworteten, dass sie sich anders verhalten hätten, als sie das sonst beim Onlineshopping tun. Da im Rahmen der Studie das tatsächliche Verhalten erfasst werden sollte und nicht davon auszugehen ist, dass diese Teilnehmer dies gezeigt haben, konnten ihre Daten im Rahmen der Auswertung nicht einbezogen werden. Als Unterschiede zu ihrem tatsächlichen Verhalten nannten Probanden unter anderem, dass sie sich zuhause mehr Zeit gelassen hätten, nur direkt bei Amazon.de bestellt hätten oder die Produkte lieber in einem Ladengeschäft gekauft hätten. Besonders das Argument bezüglich des empfundenen Zeitdrucks scheint bemerkenswert, da den Probanden theoretisch unbegrenzt Zeit gegeben wurde. Eventuell konnten sie allerdings durch die terminliche Absprache im Vorfeld auf eine Art Zeitfenster schließen, bzw. wurden durch eine angegebene ungefähre Versuchsdauer von 1-1,5 Std. unter eine Art Zeitdruck gesetzt. Zwei der Teilnehmer gaben an, sich im Rahmen des Versuchs sogar etwas unsicherer gefühlt zu haben als zuhause, da sie sich nicht ganz über das Ziel des Versuchs klar waren, bzw. sich Gedanken darüber machten, dass die personenbezogenen Daten dann auf dem Versuchsrechner gespeichert wären.

Darüber hinaus gab es Teilnehmer, bei denen sich zum Ende der Aufgabe oder im Rahmen des kurzen Interviews zeigte, dass sie die Aufgabe in irgendeiner Form falsch bearbeitet hatten. Einigen war bis zuletzt nicht klar, dass ihre eigenen Daten verwendet werden, bzw. das Produkt wirklich bestellt werden sollte. Um möglichst zweifelsfreie Aussagen zum tatsächlichen Datenschutz-Verhalten beim Onlineshopping machen zu können, wurden auch diese Teilnehmer von der Analyse ausgeschlossen. Die Tatsache, dass es an dieser Stelle im Rahmen der Explorationsstudie zu Missverständnissen kam, führte zu einer leichten Anpassung der Aufgabenstellung für die Validierungsstudie, die die Verwendung der eigenen Daten zum tatsächlichen Kauf deutlicher machen sollte. Es wird nicht davon ausgegangen, dass dies neben der Vermeidung von Missverständnissen dazu führte, dass Probanden dadurch ein anderes Shoppingverhalten zeigten. Auch im Rahmen der Validierungsstudie wurde zur Kontrolle das kurze Interview geführt und Teilnehmer, welche angaben, sich anders verhalten zu haben, von der weiteren Analyse ausgeschlossen.

Da die gestellte Aufgabe die Kriterien für eine gute Aufgabe erfüllt und die Kombination mit dem kurzen Interview dazu führt, dass nur das tatsächliche Verhalten im Rahmen des Onlineshoppings ausgewertet wird, wird davon ausgegangen, dass dieses Vorgehen eine sehr gute Basis zur Untersuchung des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping bietet.

6.1.4 Blickbewegungsanalyse

Auf Basis der im vorigen Kapitel diskutierten Kombination aus Aufgabe und Interview wurde das gezeigte Datenschutz-Verhalten technisch mittels der Blickbewegungsanalyse untersucht. Dafür wurden

im Rahmen der Explorationsstudie für alle 40 in Kapitel 3.1.1 erarbeiteten Hinweise AOI auf jede Seite jedes Webshops gelegt, bei dem die Probanden bereit waren, ihre Daten anzugeben. Aufgrund dieses enormen Aufwands wurde die Auswertung der Validierungsstudie auf die Hinweise beschränkt, die im Rahmen der Gewichtungsstudie als die acht wichtigsten resultierten. Zusätzlich dazu wurden die Hinweise als AOI gelegt, die in der vorangegangenen Studie von den Probanden am häufigsten fixiert wurden. Diese waren Preis, Produktbeschreibung und Produktbild.

Auf Basis der in Kapitel 2.5 und Kapitel 3.1.2 vorgestellten Literaturrecherche wurde zur Auswertung der auf Basis dieser AOI ausgegebenen Daten die Messgröße der Fixation verwendet. Da es an einer standardisierten Metrik diesbezüglich mangelt, musste diese Messgröße für diese Studie zunächst definiert werden. Darüber hinaus wurden Fixationen anhand ihrer spezifischen Dauer in ein Maß für einen kurzen Blick (100-200 ms) und die darüber hinaus gehende Beschäftigung (<200 ms) unterteilt. Der Gedanke dahinter war eine eventuell unterschiedliche Wichtigkeit einer kürzeren oder eben längeren Überprüfung des jeweiligen Hinweises. Abhängig davon, ob der jeweilige Proband die entsprechende AOI länger oder kürzer fixiert hätte, wäre daraufhin eine andere Bewertung des gezeigten Verhaltens erfolgt. Diese Überlegung wurde durch die Ergebnisse der Gewichtungsstudie überflüssig gemacht. Nicht nur, dass kein statistischer Unterschied zwischen der Wichtigkeit der kurzen und der längeren Betrachtung nachzuweisen war. Es ergaben sich auch keine Unterschiede in der Wichtigkeit der acht wichtigsten Hinweise. Diese Erkenntnisse führten zur Summenbildung bezüglich der Anzahl der Hinweise aus diesen acht, die von dem jeweiligen Teilnehmer/der Teilnehmerin fixiert wurden, als Maß für das gezeigte Datenschutz-Verhalten beim Onlineshopping. War ein entsprechender Hinweis auf der jeweiligen Webseite nicht vorhanden, so wurde dies äquivalent behandelt, wie ein nicht-Betrachten eines vorhandenen Hinweises.

Bezüglich der Lage der Hinweise auf einer Webseite könnte kritisiert werden, dass AOI, die sich im Zentrum eines Bildschirmes befinden, eine größere Wahrscheinlichkeit aufweisen, fixiert zu werden (Holmqvist et al., 2011). Bei Versuchen in denen man AOI als Stimuli auf dem Bildschirm präsentiert, muss dies auch abhängig von der jeweiligen Forschungsfrage beachtet werden (Holmqvist et al., 2011). In diesem Fall entspricht die Lage der Hinweise den realen Bedingungen. In dem Fall, in dem es zum Datenschutz-Verhalten einer Person gehört, die AGB zu überprüfen, wird diese Person auch notfalls nach diesen suchen. Ähnliches gilt auch für die unterschiedliche Größe der AOI. In Eye-Trackingstudien, die sich mit visueller Suche oder Verarbeitungsprozessen beschäftigen, haben Position und Größe der AOI eine ausgesprochene Relevanz (Holmqvist et al., 2011). Im Falle dieser Studie hatte der Inhalt der AOI die eigentliche Aussagekraft. Objekte, die wichtiger oder interessanter sind, werden dabei häufiger und länger fixiert als andere (Heidmann & Ziegler, 2002; Rayner, 1998). Als einschränkend kann in manchen Fällen die Größe verschiedener AOI gelten. Hier wird darauf hingewiesen, dass die natürliche Augenbewegung auch bei einer Fixation zu einem Areal von 1° Sehwinkel führt, welches fixiert wird (Jacob & Karn, 2003). Im Fall dieser Studie ergibt sich daraus eine Größe von 43,5 px (bei einem Abstand des Auges zum Bildschirm von 700 mm). Zusätzlich muss eine Ungenauigkeit der Messmethode beachtet werden. Die Genauigkeit des verwendeten Systems wird vom Hersteller mit 0.5° angegeben. Bei einer Mindestgröße der gelegten AOI von 420 px im Rahmen der Explorationsstudie und 442 px im Rahmen der Validierungsstudie sollten hier allerdings keine Einschränkungen zu erwarten sein.
Inhaltlich betrachtet gilt noch der unterschiedliche Informationsgehalt der AOI als erwähnenswert, der zu unterschiedlicher Betrachtungsdauer bezüglich der jeweiligen AOI führen kann (Rayner, 1998). Dieser kann bei dem Vergleich eines AOI wie *https* mit einem AOI wie den *Allgemeinen Geschäftsbedingungen* sicher zu Schwierigkeiten führen. Da basierend auf den Ergebnissen der

Gewichtungsstudie keine Vergleiche solcher Art durchgeführt wurden, sind auch an dieser Stelle keine Einschränkungen bezüglich der gezogenen Schlüsse zu erwarten.
Abschließend bleibt zu sagen, dass die Untersuchung der Blickbewegungen als eine objektive Methode zur Erfassung von Verhalten sehr gut im Rahmen des hier verwendeten Kontextes geeignet ist. Sie bedingt allerdings, zumindest im Rahmen der Nutzung eines, im Vergleich zu einer Eye-Trackingbrille weniger invasiven Remote-Eye-Trackers die Erhebung innerhalb einer Laboruntersuchung, die mit den genannten Einschränkungen (siehe Kapitel 2.4.3 und 3.3) einhergeht. Hinzu kommt der immense zeitliche Aufwand der Blickbewegungsanalyse (Helmert et al., 2017), der im Rahmen einer Versuchsplanung mit den gewünschten Erkenntnissen in ein Verhältnis gesetzt werden sollte (vergleiche Heidmann & Ziegler, 2002).

6.2 Diskussion des Studiendesigns der Explorations- und Validierungsstudie

Zur Erfassung tatsächlichen Verhaltens wurde ein Studiendesign konstruiert, welches nur wenigen, der in Kapitel 2.4.3 dargestellten Einschränkungen, bezüglich der Erfassung von Risikoverhalten unterliegt. So fand die Untersuchung auch in einem Labor, bzw. einer universitären Umgebung statt, die möglicherweise eine gewisse Sicherheit vermittelt. Darüber hinaus mussten die Teilnehmer auch eine Einverständniserklärung unterschreiben, in der ein sensibler Umgang mit ihren Daten zugesagt wird. Es wurde ihnen aber eine Aufgabe gestellt und die Fragebögen so dargereicht, dass der Fokus der Studie zumindest nicht klar ersichtlich war. Zur Kontrolle wurde ihnen im Anschluss an die Aufgabe die Frage gestellt, ob sie sich anders verhalten oder sicherer gefühlt hätten als das beim Onlineshopping im privaten Umfeld der Fall ist. Die wenigen Probanden, die diese Antwort nicht im Sinne der Studie beantworteten wurden nicht in die weitere Analyse einbezogen. Die Einschränkung, dass wirklich vorsichtige Personen nicht in den Daten vertreten sind (Schechter et al., 2007), wurde deshalb in Kauf genommen, weil diese Personen häufig gar keine Produkte online kaufen und somit auch nicht zur Zielgruppe dieser Studie gehörten. Im Unterschied zu anderen Studien unterlagen die Probanden während der Aufgabenbearbeitung bezüglich des online Einkaufs nicht den gängigen Einschränkungen, dass sie sich nur auf einzelnen Seiten oder gar Fake-Seiten bewegen oder nur eingeschränkte Produkte erwerben konnten. Laut Downs et al. (2006) führt das zu einer realitätsnäheren Testung. Die Sicherheit der Daten wurde in diesem Fall dadurch gewährleistet, dass der Versuch durch die Versuchsleiterin, bzw. den Versuchsleiter in dem Moment abgebrochen wurde, zu dem der Proband Daten eingeben wollte. Diese Lösung gewährleistete bis zu diesem Zeitpunkt die uneingeschränkte Nutzung des Internets, was der Produktsuche Zuhause entspricht. So war es auch möglich, dass die Teilnehmer das Risiko in Bezug auf ihre persönlichen Daten in Betracht ziehen mussten und nicht vorgegebener, fremder Personendaten, wie das bei der Nutzung von Fake-Accounts der Fall ist. An dieser Stelle könnte eingewendet werden, dass auf einige der Hinweise, wie vor allem die Datenschutzerklärungen und AGB erst nach der ersten Dateneingabe explizit hingewiesen wird. Hier wird sich auf die Studie von Whalen und Inkpen (2005) berufen, die zu dem Schluss kamen, dass nach der Dateneingabe (in ihrem Fall dem Einloggen auf einer online-banking Seite), ein Zustand von Sicherheit entsteht, während der sich der Nutzer entspannt und aufhört nach Hinweisen zu schauen. Darüber hinaus wären zu diesem Zeitpunkt die Daten auch bereits eingegeben. Für ein nachträgliches Schauen nach AGB oder Datenschutzerklärungen kann es zu diesem Zeitpunkt schon zu spät sein (Boos, 2015). Zwei Einschränkungen bleiben allerdings bestehen. Hätten die Teilnehmer nicht ihre tatsächlichen Daten, sondern z. B. Phantasienamen verwenden und somit nicht ihre eigenen Daten in Gefahr bringen wollen, so wäre dies im Rahmen des Versuchs unbemerkt geblieben. Neben der Tatsache, dass die Verwendung von falschen Daten im Rahmen des

Onlineshoppings wenig sinnvoll ist, möchte man ein Produkt auch tatsächlich erhalten, ist davon auszugehen, dass sich diese Probanden bei der Aufgabenbearbeitung anders verhalten und dies im Rahmen des Interviews angemerkt hätten. Dies gilt auch für Teilnehmer und Teilnehmerinnen, die möglicherweise, aufgrund der in Aussicht gestellten Aufwandsentschädigung, die Aufgabe beendeten, obwohl sie das eigentlich lieber nicht getan hätten.

In der Studie von Downs et al. (2006) zeigte sich, dass die Teilnehmer Hinweise falsch interpretierten. Hargittai (2007) beschreibt darüber hinaus, dass das, was die Nutzer überprüfen, auch nicht notwendigerweise richtig ist. Um damit umgehen zu können, müssten die Nutzer sich aber zunächst darüber im Klaren sein, dass Falschinformationen existieren können und somit eine gewisse Skepsis innehaben. Im nächsten Schritt müssten sie wissen, wie sie Informationen bezüglich der Richtigkeit, bzw. der Quelle der Informationen sammeln können, was nicht immer trivial ist. Im Rahmen der hier vorgestellten Studien kann über die Richtigkeit der Interpretationen, bzw. den Wahrheitsgehalt der betrachteten Hinweise keine Aussage gemacht werden.

6.3 Diskussion der Stichproben im Rahmen der Explorations- und der Validierungsstudien

Die beiden Stichproben, denen die gefundenen Erkenntnisse zugrunde liegen, hatten aus verschiedenen Gründen einen eingeschränkten Umfang. Einer dieser Gründe lag in den begrenzten finanziellen Mitteln, die für die Durchführung der Studie und somit für die Aufwandsentschädigungen für Probanden zu Verfügung stand. Ein anderer Grund war der bereits erwähnte große Aufwand, den sowohl die Erhebung mit bis zu 1,5 Stunden pro Teilnehmer, als auch die Analyse der Blickbewegungen so vieler Probanden auf jeweils unterschiedlichen Webseiten mit sich bringt. Darüber hinaus unterlag die Stichprobe einer Einschränkung, die erst im Rahmen der Validierungsstudie deutlich und im Vorfeld nicht bedacht wurde. Bei Probanden, die eine Sehhilfe benötigen, kann es wie bereits in Kapitel 2.5.5 beschrieben zu Störungen der Reflektion des vom Blickbewegungssystems gesendeten Infrarotsignals kommen. Da die Altersverteilung der Explorationsstudie einen hohen Anteil junger Probandinnen und Probanden aufwies, sollte im Rahmen der Validierungsstudie darauf geachtet werden, mehr ältere Menschen für die Teilnahme zu gewinnen. Die Schwierigkeit war, dass es ab einem gewissen Alter kaum noch Menschen gibt, die nicht auf eine Sehhilfe angewiesen sind. Aus über 80 persönlichen Anfragen ergaben sich trotz überaus großer Bereitschaft nur zwei Probanden, deren Blickbewegungen aufgezeichnet werden konnten.
Die zusammengelegten Stichproben ergaben aber eine Gesamtstichprobe, die für die wesentlichen Tests in Bezug auf die beiden Modelle ausreichend groß war. In der Zusammenlegung der beiden Stichproben wird kein methodisches Problem gesehen. Im Rahmen von Meta-Analysen, z. B. bei medizinischen Untersuchungen sind sie gängige Praxis, unterliegen aber einigen Auflagen (Blettner, Sauerbrei, Schlehofer, Scheuchenpflug & Friedenreich, 1999). So müssen für eine zusammengelegte Analyse (*pooled analysis*) die verwendeten Variablen einheitlich definiert und die einbezogenen Studien möglichst ähnlich sein (Blettner et al., 1999). Die Zusammenlegung von Rohdaten für eine retrospektive Analyse entspricht dabei einer Meta-Analyse Typ III (Blettner et al., 1999; Leonhart & Maurischat, 2004). Leonhart und Maurischat (2004) stellen Gründe dar, warum diese erstrebenswerte Art der Meta-Analyse häufig nicht möglich ist. Dazu gehören Einschränkungen bei der Weitergabe von Daten an Dritte, sei es durch vorangegangene Einverständniserklärungen, bei denen dies im Vorfeld nicht bedacht und die Möglichkeit miteinbezogen wurde oder aufgrund der Situation bezüglich der Nutzungsrechte. Teilweise liegen die Gründe auch in der erschwerten, nachträglichen Erreichbarkeit der Verantwortlichen oder

dem fehlenden Zugriff auf die Daten (Leonhart & Maurischat, 2004). Jacob & Karn (2003) weisen in Bezug auf Blickbewegungsanalyse darauf hin, dass schon nur leicht unterschiedliche Parameter innerhalb des Algorithmus einer automatisierten Fixationserkennung dazu führen, dass die Messgrößen zwischen zwei Studien nicht mehr vergleichbar sind. Im Rahmen dieser Studie kommen all diese Punkte allerdings nicht zum Tragen, da in beiden Fällen sowohl die gleichen Parameter, das gleiche Studiendesign, das gleiche Equipment und auch derselbe Algorithmus verwendet wurden.
Neben der Größe ist die Zusammensetzung der Stichprobe ein häufig diskutierter Punkt. Um statistisch haltbare Aussagen und Rückschlüsse auf eine übergeordnete Population machen zu können, müsste die Stichprobenauswahl zufallsgesteuert vonstattengehen. Dies würde bedeuten, dass jedes Individuum der Population theoretisch die gleiche Chance haben müsste, an der Studie teilzunehmen (Döring & Bortz, 2016). Bei einer Population von Menschen, die Produkte online erwerben, die fast 80% der deutschen Bevölkerung beträgt (Bitkom, 2017b; Initiative D21, 2018) in Kombination mit einer Laborstudie, ist das nahezu unmöglich. Entgegen dieser mathematischen-statistischen Position hierzu steht eine eher erkenntnistheoretische Position (Döring & Bortz, 2016). Bei dieser steht der sogenannte Bewährungsgrad von Hypothesen und Theorien im Vordergrund. Ein gefundener statistischer Zusammenhang kann somit zwar vielleicht nicht übertragbar auf eine Grundgesamtheit sein, er gibt aber einen ersten Hinweis auf den Bewährungsgrad der Hypothese oder Theorie (Döring & Bortz, 2016). Dieser steigt, wird dieser Zusammenhang in weiteren Studien repliziert (Döring & Bortz, 2016).

7 Fazit und Ausblick

Die Tatsache, dass im Kontext des Datenschutzes eine Inkonsistenz zwischen Aussagen von Nutzern und deren Verhalten existiert, führt zur Notwendigkeit der Erfassung tatsächlichem Verhaltens im Zuge der Forschung auf diesem Gebiet. Die größte Schwierigkeit stellt dabei die Schaffung einer möglichst realistischen Situation dar, in der die Teilnehmer ein gewisses Risiko wahrnehmen, gleichzeitig aber keinem tatsächlichen Risiko ausgesetzt sind.
Hieraus ergab sich *Forschungsfrage 1*: *Wie lässt sich tatsächliches Datenschutz-Verhalten beim Onlineshopping empirisch erfassen?*
Die erste Frage, die sich dabei stellt entspricht *Forschungsfrage 1a: Wie kann tatsächliches Datenschutz-Verhalten beim Onlineshopping operationalisiert werden?*
Um diese beantworten zu können, wurde auf den dargestellten Stand der Forschung und Technik zurückgegriffen. Dieser behandelte die Fragen, welche Risiken in diesem Rahmen existieren, welche Möglichkeiten der Absicherung es dagegen gibt und wie Menschen tatsächlich mit diesen Risiken umgehen. Im Speziellen wurde erörtert, welche Methoden und Messgrößen zur Erfassung von Risiko-Verhalten in diesem Kontext in bisherigen Studien verwendet werden. Da sich diese als aussichtsreiche und einzige Methode zur objektiven und verzerrungsfreien Beobachtung von Verhalten herausstellte, wurde die Blickbewegungsanalyse im Detail dargestellt. Aus den dargestellten Erkenntnissen ließ sich bezüglich Forschungsfrage 1 ableiten, dass die Überprüfung von Hinweisen, die eine Aussage über den Umgang mit personenbezogenen Daten von Seiten des Webshops machen, ein geeignetes Verhalten zum Schutz der personenbezogenen Daten darstellt, welches sich im Rahmen einer Blickbewegungsanalyse objektiv beobachten lässt.
Zur anschließenden Beantwortung von *Forschungsfrage 1b: Wie kann erhobenes Verhalten für weitere Analysen quantifiziert werden?* wurden entsprechende Hinweise gesammelt und eine geeignete Messgröße im Rahmen der Blickbewegung identifiziert. Um die gefundene Anzahl an Hinweisen einschränken zu können, wurde eine Expertenbefragung durchgeführt. Diese hatte die Gewichtung der Hinweise und die Bewertung einer entsprechenden notwendigen Betrachtungsdauer als zusätzliches Ziel. Es ergaben sich acht wichtigste Hinweise, die sich in ihrer Wichtigkeit und notwendigen Betrachtungsdauer nicht unterscheiden. Die Summe der betrachteten Hinweise aus diesen acht wichtigsten vor Eingabe der persönlichen Daten im Zuge eines Online-Einkaufs stellt demnach die Antwort auf Forschungsfrage 1b dar.
Eine Analyse bezüglich anderer Studien in diesem Kontext und deren Limitation und Einschränkungen führten zur Ableitung von Anforderungen, wie möglichst breit verteilte Stichproben, Standardisierung der Methoden oder einer kontextspezifischen Erhebungssituation, die ein Risiko impliziert ohne, dass ein solches existiert. Diese Erkenntnisse beantworteten *Forschungsfrage 1c: Welche Anforderungen bestehen an eine solche empirische Erhebung?*
In Bezug auf die *Forschungsfragen 2: Welche personenbezogenen Faktoren haben einen Einfluss auf das tatsächliche Datenschutz-Verhalten beim Onlineshopping?* und *3: Inwieweit lässt sich das tatsächliche Datenschutz-Verhalten beim Onlineshopping mit Hilfe der gefundenen Einflussfaktoren vorhersagen?* fand die Beantwortung in mehreren Schritten, mit Hilfe zweier Studien statt. Auf Basis eines aus der Literatur abgeleiteten Arbeitsmodells wurde eine Explorationsstudie durchgeführt, die die Erkenntnisse zu Forschungsfrage 1 adressierte und das Potential unterschiedlicher Prädiktoren untersuchte. Basierend darauf wurde das Arbeitsmodell angepasst, bzw. in zwei überprüfbare Modelle aufgeteilt. Die Diskussion der verwendeten Methodik führte zu geringen Anpassungen bezüglich der im Anschluss durchgeführten Validierungsstudie.

Die Ergebnisse der Studien zeigen, dass die Teilnehmer nur wenig auf Hinweise schauten, die ihnen Auskunft darüber hätten geben können, wie von Seiten des jeweiligen Webshops mit personenbezogenen Daten umgegangen wird. Sie gehen damit ein hohes Risiko dafür ein, dass ihre persönlichen Daten in die falschen Hände geraten können.
Bezüglich Forschungsfrage 2 erwies sich ausschließlich die Variable Alter als signifikanter, personenbezogener Prädiktor für das tatsächliche Datenschutz-Verhalten beim Onlineshopping. Der Anteil erklärter Varianz, der im Rahmen von Forschungsfrage 3 gefragt war, stellte sich dabei als gering dar. Die per Fragebogen erfragten Variablen bezüglich der Handlung Daten anzugeben, ohne Datenschutzerklärungen angeschaut zu haben (wahrgenommenes Risiko, erwarteter Nutzen und die Wahrscheinlichkeit) konnten keinen signifikanten Beitrag zur Überprüfung des tatsächlichen Verhaltens beitragen. Dieses Ergebnis entspricht dem Privacy Paradoxon und weist konform damit auf die Notwendigkeit der Erhebung des tatsächlichen Datenschutz-Verhaltens im Rahmen weiterer Forschung hin.
Es lässt sich sagen, dass im Rahmen der Arbeit alle Forschungsfragen beantwortet wurden. Das erarbeitete Studiendesign und die Operationalisierung des tatsächlichen Datenschutz-Verhaltens beim Onlineshopping sind als Basis für weitere Studien geeignet. Denkbar ist hier die Überprüfung des Prädiktionsvermögens von Faktoren, die nicht in der Person des jeweiligen Nutzers liegen, wie zum Beispiel das empfundene Vertrauen in Technik oder in den jeweiligen Anbieter des Webshops. Auch die Erfassung der Persönlichkeit der Nutzer, deren Selbstwirksamkeit oder Akzeptanz könnte in Verbindung mit der Erfassung des tatsächlichen Verhaltens zu aussagekräftigen Ergebnissen führen.
Darüber hinaus kann die Identifikation des Alters als signifikanter Prädiktor des tatsächlichen Verhaltens eine Basis für die Ableitung entsprechender Nutzerunterstützungen bieten. Im Rahmen der Entwicklung entsprechender Sicherheitssysteme ist es notwendig, etwas über die Charakteristika der Nutzer und ihr potentielles Verhalten zu wissen (Cranor, 2008; Figner & Weber, 2011).
Ohne aber neue Studien mit dem erarbeiteten Studiendesign durchzuführen, kann schon die Auswertung der bereits erhobenen Daten weitere Erkenntnisse bringen. Interessant wäre hier z. B., die Webseiten bei denen die Probanden gekauft hätten auf deren Vertrauenswürdigkeit zu prüfen, oder sie diesbezüglich von Experten einschätzen zu lassen, um der Frage auf den Grund zu gehen, ob bereits mit der Überprüfung von nur vier Hinweisen ein ausreichendes Maß an Sicherheit erreicht werden kann.
Im Weiteren wäre es möglich, die Blickbewegungsaufzeichnungen zu nutzen um Aussagen darüber machen zu können, wie die Teilnehmer zu dem jeweiligen Webshop gelangten, an welchen Hinweisen sich orientierten, in wieweit sie Suchmaschinen oder Preisvergleich-Anbieter verwendeten, ob sich Abbruchkriterien auf den Seiten ermitteln lassen, bei denen sich gegen einen Kauf entschieden wurde und ob diese eventuell im Zusammenhang mit Datensicherheit stehen. Hier wäre es eventuell denkbar das Blickverhalten z. B. mittels Markov-Modellen oder –Ketten abzubilden um Entscheidungsstrategien darzustellen oder Vorhersagen machen zu können (Schlick et al., 2018).
Ein weiterer Fokus der Auswertung könnte auf der Auswahl der Produkte liegen, für die sich die Probanden interessiert hatten. Diesbezüglich könnte untersucht werden, ob sich eventuell Cluster bilden lassen, die möglicherweise mit Auswahlstrategien oder dem Datenschutz-Verhalten in Zusammenhang zu bringen sind. Auch das Clustern der personenbezogenen Daten nach Vorbild der bereits erwähnten Milieu-Studie (SINUS-Institut Heidelberg, 2012) könnte zu weiterführenden Aussagen bezüglich einer Prädiktion oder dem Zusammenhang mit Strategien jedweder Art führen.
Eine Betrachtung der tatsächlich verwendeten Hinweise, in Bezug auf deren Lage, Größe, Farben oder anderen Messgrößen könnte Ansatzpunkte für Gestaltungshinweise bieten. So erwähnt Waldman (2018), dass die heutigen Datenschutzregelungen schlecht gestaltet sind und deren Inhalte von Juristen für Juristen gemacht wären. Im Rahmen einer Studie auf Basis von 191 Screenshots fand er heraus, dass

deren Design Einfluss auf das Verhalten der Nutzer hat. Das bedeute allerdings auch, dass ein gutes Design Nutzer dazu bewegen kann sich auf ungünstige Konditionen einzulassen (Waldman, 2018).
Wie bereits erwähnt, steht den Nutzern hauptsächlich die Webseite des Anbieters zu Verfügung um sich ein Bild bezüglich des Umgangs mit Datenschutz zu machen. Gestaltungshinweise können ebenso dem Anbieter dazu dienen, seine Vertrauenswürdigkeit besser darzustellen, um Privacy Bedenken potentieller Kunden entgegenzuwirken (Buxmann, 2015). Wang et al. (2004) empfehlen dies vor allem kleinen Online-Händlern. Im Rahmen eines Marktes, in dem Organisationen Informationen über ihre Nutzer brauchen (Olivero & Lunt, 2004), müssen Internetanbieter in die Verbesserung ihrer Vertrauenswürdigkeit investieren. Ahrholdt (2010) geht davon aus, dass eine auf die Charakteristika des jeweiligen Nutzers zugeschnittene Darstellung von Hinweisen auf der Webseite die Zahl der Kunden erhöhen kann. An dieser Stelle sei auf den im Rahmen dieser Studie signifikanten Einfluss der Variable Alter hingewiesen. Laut Bhatnagar und Ghose (2004) kann es für Firmen eine aussichtsreiche Strategie sein, ihre teilweise ängstlichen Kunden zu bilden. In den letzten Jahren wurde viel für den Schutz der Daten getan, es wurde nur versäumt die Nutzer darüber zu informieren (Bhatnagar & Ghose, 2004).
Wambach (2017) erwähnt dagegen die Notwendigkeit durch Bildungsmaßnahmen, ein grundlegendes Gefahrenbewusstsein auf Seiten der Verbraucher zu schaffen. Dabei warnen er und seine Kollegin besonders vor der Tatsache, dass weniger Unternehmen immer mehr Informationen über uns Nutzer sammeln (Wambach & Bräunlich, 2016). Wu et al. (2006) konnten im Rahmen ihrer Studie nachweisen, dass das Vorhandensein eines Tutorials die Sicherheit des Verhaltens erhöhte.
Obwohl diese Variable in der vorliegenden Arbeit keinen signifikanten Beitrag zum Verhalten leistete, wird davon ausgegangen, dass das Wissen der Nutzer verbessert werden muss (Bitkom, 2017a; Downs et al., 2006). Dabei gehen van Dijk und van Deursen (2010) davon aus, dass jüngere Nutzer eher Informationen und strategische Fähigkeiten und die älteren operative und formalen Fähigkeiten brauchen um die Verfahren zu lernen, die benötigt werden um den Datenschutz zu gewährleisten. Sowohl LaRose et al. (2008), als auch West (2008) erwähnen in Bezug auf die Verbesserung der Sicherheit die Möglichkeit nicht nur auf das Risiko hinzuweisen, sondern gutes Verhalten zu belohnen um die Motivation hierfür zu steigern.
Darüber hinaus sollte sich laut dem Institut für angewandte Sozialwissenschaften (2014) und auch Norberg et al. (2007) die Politik und die Justiz angesprochen fühlen.
Interessant hierbei ist die Aussage des Erfinders des Internets selbst, Professor Tim Berners-Lee am 28. Geburtstag seiner Erfindung: Er sieht den Verlust der persönlichen Daten als eine wesentliche Herausforderung (Berners-Lee, 2017). Seiner Meinung nach verzichten wir bei der Freigabe unserer Daten auf die Benefits, die es hätte, wenn wir direkte Kontrolle über unsere Daten und darüber hätten, wann und mit wem wir welche Daten teilen, bzw. vielmehr, welche Art von Daten wir nicht teilen wollen. Er erläutert, wie die Datensammlung von Firmen und Regierungen dazu führen kann, dass Datenschutzrechte verletzt, Blogger verhaftet oder getötet und politische Gegner überwacht werden. Diese Entwicklung verhindere dass das Internet als Raum genutzt wird, in dem man sich frei über wichtige Themen informieren kann. Seine Lösung, deren Entwicklung Professor Tim Berners-Lee am MIT selbst leitet, sieht vor, dass die persönlichen Daten eines jeden Nutzers auf einer Plattform liegen und der Nutzer einzelnen Anbietern, Apps oder Personen Zugang gewähren kann, während die Daten selbst aber bei ihm verbleiben (The Solid Project, o.D.). Möglicherweise gelingt ihm damit eine erneute weltverändernde Erfindung.

Literaturverzeichnis

Acquisti, A. & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy Magazine, 3* (1), 26–33. https://doi.org/10.1109/MSP.2005.22

Ahrholdt, D. (2010). *Erfolgsfaktoren einer E-Commerce-Website: Empirische Identifikation vertrauensfördernder Signale im Internet-Einzelhandel* (Betriebswirtschaftliche Aspekte lose gekoppelter Systeme und Electronic Business, 1. Auflage 2010). Wiesbaden: Springer Fachmedien.

Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior. In Action *Control - From Cognition to Behavior* (S. 11–39). Zugriff am 03.08.2018. Verfügbar unter http://link.springer.com/chapter/10.1007/978-3-642-69746-3_2

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50* (2), 179–211. Zugriff am 23.05.2016. Verfügbar unter http://www.sciencedirect.com/science/article/pii/074959789190020T

Alba, J. W. & Hutchinson, J. (2000). Knowledge calibration: What consumers know and what they think they know. *Journal of consumer research, 27* (2), 123–156. Zugriff am 31.05.2017. Verfügbar unter https://academic.oup.com/jcr/article/27/2/123/1785989

Amichai-Hamburger, Y. & Vinitzky, G. (2010). Social network use and personality. *Computers in Human behavior, 26* (6), 1289–1295. Zugriff am 04.09.2013. Verfügbar unter http://www.sciencedirect.com/science/article/pii/S0747563210000580

Anderson, C. L. & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly, 34* (3), 613-A15. Zugriff am 20.02.2017. Verfügbar unter http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=52546047&site=ehost-live

Arbeitsgemeinschaft Online Forschung e.V. (2013). *internet facts 2013-04.* Zugriff am 04.11.2018. Verfügbar unter https://www.agof.de/download/Downloads_Internet_Facts/Downloads_Internet_Facts_2013/Downloads_Internet_Facts_2013-04/04-2013_AGOF%20internet%20facts%202013-04.pdf?x81622

Arbeitsgemeinschaft Online Forschung e.V. (2015). *internet facts 2015-05.* Zugriff am 04.11.2018. Verfügbar unter https://www.agof.de/download/Downloads_Internet_Facts/Downloads_Internet_Facts_2015/Downloads_Internet_Facts_2015-05/05-2015_AGOF%20internet%20facts%202015-05.pdf?x81622

Atkinson, J. W. (1957). Motivational determinants of risk-taking behavior. *Psychological Review, 64* (6, Pt.1), 359–372. https://doi.org/10.1037/h0043445

Backhaus, K., Erichson, B., Plinke, W. & Weiber, R. (2016). *Multivariate Analysemethoden. Eine anwendungsorientierte Einführung* (14., überarbeitete und aktualisierte Auflage). Berlin: Springer Gabler. https://doi.org/10.1007/978-3-662-46076-4

Badke-Schaub, P., Hofinger, G. & Lauche, K. (Hrsg.). (2008). *Human factors - Psychologie sicheren Handelns in Risikobranchen* (1. Aufl.). Heidelberg: Springer Medizin Verlag.

Bartsch, S., Boos, C., Dyck, D., Henhapl, B., Schwarz, C., Theuerling, H. et al. (2014). Unterstützung für ein risikobewusstes Verhalten im Internet. In A. Zeising, C. Draude, H. Schelhowe & S. Maß (Hrsg.), *Vielfalt der Informatik: Ein Beitrag zu Selbstverständnis und Außenwirkung* (1. Aufl., S. 168–171). Bremen. Zugriff am 05.11.2018. Verfügbar unter http://elib.suub.uni-bremen.de/edocs/00104194-1.pdf

Bäuerlein, A.-L., Braun, J. & Ziemek, M. (2013). *Evaluation eines Online-Quiz zur IT-Sicherheits-Expertise*. Technische Universität Darmstadt, Darmstadt.

Becker, L. (2015). *Einfluss von Internetsicherheit-Expertise auf die Einschätzung der Vertrauenswürdigkeit von Webseiten*. Studienarbeit. Technische Universität Darmstadt, Darmstadt.

Beresford, A. R., Kübler, D. & Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. *Economics Letters, 117* (1), 25–27. Zugriff am 23.05.2016. Verfügbar unter http://www.sciencedirect.com/science/article/pii/S0165176512002182

Berners-Lee, T. (2017, 12. März). *Three challenges for the web, according to its inventor,* World Wide Web Foundation. Zugriff am 23.04.2018. Verfügbar unter https://webfoundation.org/2017/03/web-turns-28-letter/

Bernoulli, D. (1954). Exposition of a new theory on the measurement of risk. *Econometrica: Journal of the Econometric Society, 22* (1), 23–36. Zugriff am 15.08.2012. Verfügbar unter http://www.jstor.org/stable/10.2307/1909829

Berufsverband E-Commerce und Versandhandel Deutschland. (01/2018). *E-Commerce – der neue Nahversorger?* Zugriff am 07.03.2018. Verfügbar unter https://de.statista.com/statistik/daten/studie/71568/umfrage/online-umsatz-mit-waren-seit-2000/

Bhatnagar, A. & Ghose, S. (2004). Segmenting consumers based on the benefits and risks of Internet shopping. *Journal of Business Research, 57* (12), 1352–1360. Zugriff am 08.09.2015. Verfügbar unter http://www.sciencedirect.com/science/article/pii/S0148296303000675

Bhattacherjee, A. & Sanford, C. (2009). The intention-behaviour gap in technology usage: the moderating role of attitude strength. *Behaviour and Information Technology, 28* (4), 389–401.

Bhattacherjee, A. (2014). Individual Trust in Online Firms. Scale Development and Initial Test. *Journal of Management Information Systems, 19* (1), 211–241. https://doi.org/10.1080/07421222.2002.11045715

Birmingham, E., Bischof, W. F. & Kingstone, A. (2009). Get real! Resolving the debate about equivalent social stimuli. *Visual Cognition, 17* (6-7), 904–924. https://doi.org/10.1080/13506280902758044

Biswas, D. & Biswas, A. (2004). The diagnostic role of signals in the context of perceived risks in online shopping: do signals matter more on the web? *Journal of interactive marketing, 18* (3), 30–45. Zugriff am 01.02.2017. Verfügbar unter http://www.sciencedirect.com/science/article/pii/S1094996804701097

Bitkom. (2017a). *Cybercrime: Jeder zweite Internetnutzer wurde Opfer.* Zugriff am 17.04.2018. Verfügbar unter https://www.bitkom.org/Presse/Presseinformation/Cybercrime-Jeder-zweite-Internetnutzer-wurde-Opfer.html

Bitkom. (12/2017b). *Trends im E-Commerce - So shoppen die Deutschen.* Zugriff am 07.03.2018. Verfügbar unter https://de.statista.com/statistik/daten/studie/76228/umfrage/anteil-der-online-shopper-an-den-internetnutzern-in-deutschland-seit-2002/

Blais, A.-R. & Weber, E. U. (2006). A Domain-Specific Risk-Taking (DOSPERT) Scale for Adult Populations. *Judgment and Decision Making, 1* (1), 33–47. Zugriff am 25.01.2012.

Blake, B. F., Neuendorf, K. A. & Valdiserri, C. M. (2003). Innovativeness and variety of internet shopping. *Internet Research, 13* (3), 156–169. Zugriff am 30.05.2017. Verfügbar unter http://www.emeraldinsight.com/doi/pdf/10.1108/10662240310478187

Blettner, M., Sauerbrei, W., Schlehofer, B., Scheuchenpflug, T. & Friedenreich, C. (1999). Traditional reviews, meta-analyses and pooled analyses in epidemiology. *International Journal of Epidemiology, 28* (1), 1–9. https://doi.org/10.1093/ije/28.1.1

Blumer, T. & Doering, N. (2012). Are we the same online? The expression of the five factor personality traits on the computer and the Internet. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 6* (3). Zugriff am 04.09.2013. Verfügbar unter http://www.cyberpsychology.eu/view.php?cisloclanku=2012121201

Boos, C. (2015). *Verbraucher-und Datenschutz bei Online-Versanddiensten. Automatisierte Einschätzung der Vertrauenswürdigkeit durch ein Browser-Add-on*. Zugl.: Kassel, Diss., 2015. Zugriff am 23.05.2016. Verfügbar unter http://d-nb.info/108026776X/34

Bortz, J. (2005). *Statistik: Für Human-und Sozialwissenschaftler* (6. Aufl.). Heidelberg: Springer-Verlag.

Bravo-Lillo, C., Cranor, L., Downs, J. & Komanduri, S. (2011). Bridging the gap in computer security warnings: a mental model approach. *Security & Privacy, IEEE* (99), 1.

Brown, J. W. & Braver, T. S. (2007). Risk prediction and aversion by anterior cingulate cortex. *Cognitive, Affective, & Behavioral Neuroscience, 7* (4), 266–277. https://doi.org/10.3758/CABN.7.4.266

Bundesamt für Sicherheit in der Informationstechnik. (o.D.a). *IT-Grundschutz - Basis für Informationssicherheit.* Zugriff am 28.09.2018. Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/allgemein/einstieg/01001.html

Bundesamt für Sicherheit in der Informationstechnik. (o.D.b). *Worauf beim Online-Einkauf zu achten ist.* Zugriff am 01.09.2018. Verfügbar unter https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/EinkaufenImInternet/OnlineShoppingbeachten/OnlineShoppingbeachten_node.html

Bundesamt für Sicherheit in der Informationstechnik. (o.D.c). *Zwölf Maßnahmen zur Absicherung gegen Angriffe aus dem Internet.* Zugriff am 01.09.2018. Verfügbar unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/Massnahmen_gegen_Internetangriffe.html?nn=6596218

Bundesamt für Sicherheit in der Informationstechnik. (2017a). *Online-Shops: Einschätzung der Seriosität und Sicherheit,* Bundesamt für Sicherheit in der Informationstechnik. Verfügbar unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Sicherheit_Onlineshopping_22112017.html

Bundesamt für Sicherheit in der Informationstechnik. (2017b). *Online-Skimming: 1.000 deutsche Online-Shops betroffen.* Zugriff am 18.04.2018. Verfügbar unter https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/Skimming_09012017.html

Bundeskriminalamt. (2017, 17. August). *Bundeslagebild Cybercrime 2016.* Zugriff am 13.03.2018. Verfügbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html

Bundeskriminalamt. (2018). *Internetkriminalität/Cybercrime.* Zugriff am 07.03.2018. Verfügbar unter https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html;jsessionid=385230039A51A4C805E33DC202498D1A.live2302

Business Insider Inc, Galant, G. (Mitarbeiter). (2010). *Online Privacy Is The New 'Programming A VCR'.* Zugriff am 04.11.2018. Verfügbar unter https://www.businessinsider.com/online-privacy-is-the-new-programming-a-vcr-2010-4?IR=T

Buxmann, P. (2015). Der Wert von Daten und Privatsphäre – empirische Ergebnisse aus Anwender- und Anbietersicht. *Wirtschaftsdienst, 95* (12), 810–814. Zugriff am 07.03.2018. Verfügbar unter https://archiv.wirtschaftsdienst.eu/jahr/2015/12/verbraucher-und-digitale-welt-wo-geht-die-reise-hin/search/wei%C3%9F/20/

Byrnes, J. P., Miller, D. C. & Schafer, W. D. (1999). Gender differences in risk taking: A meta-analysis. *Psychological bulletin, 125* (3), 367. Zugriff am 28.02.2013. Verfügbar unter http://psycnet.apa.org/journals/bul/125/3/367/

Campbell, A. J. (1997). Relationship marketing in consumer markets. A comparison of managerial and consumer attitudes about information privacy. *Journal of Direct Marketing, 11* (3), 44–57. https://doi.org/10.1002/(SICI)1522-7138(199722)11:3<44::AID-DIR7>3.0.CO;2-X

Carlson, J. P., Bearden, W. O. & Hardesty, D. M. (2007). Influences on what consumers know and what they think they know regarding marketer pricing tactics. *Psychology & Marketing, 24* (2), 117–142. Zugriff am 30.05.2017. Verfügbar unter http://onlinelibrary.wiley.com/doi/10.1002/mar.20155/full

Chadwick-Dias, A., McNulty, M. & Tullis, T. (2003). Web Usability and Age: How Design Changes Can Improve Performance. In Proceedings *of the 2003 Conference on Universal Usability* (CUU '03, S. 30–37). New York, NY, USA: ACM. Zugriff am 26.01.2015. Verfügbar unter http://doi.acm.org/10.1145/957205.957212

Chambers, C. P. & Echenique, F. (2016). *Revealed preference theory* (Econometric Society monographs, Bd. 56). Cambridge: Cambridge University Press.

Chou, N., Ledesma, R., Teraguchi, Y., Boneh, D. & Mitchell, J. C. (2004). Client-side defense against Web-based identity theft. *Proceedings of the 11th Annual Network and Distributed System Security Symposium.* Zugriff am 27.01.2018.

Cortina, J. M. (1993). What is coefficient alpha? An examination of theory and applications. *Journal of applied psychology, 78* (1), 98. Zugriff am 01.08.2012. Verfügbar unter http://psycnet.apa.org/journals/apl/78/1/98/

Cranor, L. F. (2008). A framework for reasoning about the human in the loop. In Proceedings *of the 1st Conference on Usability, Psychology, and Security* (Bd. 1, S. 1).

(2018). Datenschutz-Grundverordnung. DSGVO. Zugriff am 29.08.2018. Verfügbar unter https://dsgvo-gesetz.de/

Debel, A., Feldbusch, W., Ghafarian, M. & Moghaddamkia, H. (2013). *Evaluation eines Online-Quiz zur IT-Sicherheits-Expertise*. Tutorium. Technische Universität Darmstadt, Darmstadt.

Delabarre, E. B. (1898). A method of recording eye-movements. *The American Journal of Psychology, 9* (4), 572–574. Zugriff am 07.07.2016. Verfügbar unter http://www.jstor.org/stable/1412191

Demeter, P. (2015). Near Field Communication im Handel: Expertenbefragung mittels Delphi-Methode. *HMD Praxis der Wirtschaftsinformatik, 52* (2), 240–248.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. (o.D.). *Eingriffe in das Recht auf informationelle Selbstbestimmung nur auf der Grundlage eines Gesetzes, das auch dem Datenschutz Rechnung trägt (Volkszählungsurteil)*. Zugriff am 27.01.2018. Verfügbar unter https://www.bfdi.bund.de/DE/Datenschutz/Themen/Melderecht_Statistiken/VolkszaehlungArtikel/151283_VolkszaehlungsUrteil.html

Dodge, R. & Cline, T. S. (1901). The angle velocity of eye movements. *Psychological Review, 8* (2), 145. Zugriff am 07.07.2016. Verfügbar unter http://psycnet.apa.org/journals/rev/8/2/145/

Döring, N. & Bortz, J. (2016). *Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften* (Springer-Lehrbuch, 5. vollständig überarbeitete, aktualisierte und erweiterte Auflage). Berlin: Springer. https://doi.org/10.1007/978-3-642-41089-5

Dörner, C. (2015). *Verhalten von Internetnutzern bei der Einschätzung der Vertrauenswürdigkeit von Webseiten*. Studienarbeit. Technische Universität Darmstadt, Darmstadt.

DOSPERT.org. Zugriff am 08.06.2018. Verfügbar unter https://sites.google.com/a/decisionsciences.columbia.edu/dospert/r-package

Downs, J. S., Holbrook, M. B. & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. In Proceedings *of the second symposium on Usable privacy and security* (S. 79–90).

Duchowski, A. T. (2002). A breadth-first survey of eye-tracking applications. *Behavior Research Methods, Instruments, & Computers, 34* (4), 455–470. Zugriff am 22.02.2017. Verfügbar unter http://link.springer.com/article/10.3758/BF03195475

Duden. (2018a). *Definition Daten,* Bibliographisches Institut GmbH. Zugriff am 27.10.2018. Verfügbar unter http://www.duden.de/rechtschreibung/Daten#b2-Bedeutung-2

Duden. (2018b). *Definition Datenschutz,* Bibliographisches Institut GmbH. Zugriff am 27.10.2018. Verfügbar unter http://www.duden.de/rechtschreibung/Datenschutz

Duden. (2018c). *Definition Datensicherheit,* Bibliographisches Institut GmbH. Zugriff am 27.10.2018. Verfügbar unter http://www.duden.de/suchen/dudenonline/datensicherheit

Duden. (2018d). *Definition Handlung,* Bibliographisches Institut GmbH. Zugriff am 27.10.2018. Verfügbar unter http://www.duden.de/rechtschreibung/Handlung

Duden. (2018e). *Definition Hinweis,* Bibliographisches Institut GmbH. Zugriff am 27.10.2018. Verfügbar unter https://www.duden.de/rechtschreibung/Hinweis

Duden. (2018f). *Definition Onlineshopping,* Bibliographisches Institut GmbH. Zugriff am 27.10.2018. Verfügbar unter http://www.duden.de/rechtschreibung/Onlineshopping

Duden. (2018g). *Definition Risiko,* Bibliographisches Institut GmbH. Zugriff am 27.10.2018. Verfügbar unter http://www.duden.de/rechtschreibung/Risiko

Duden. (2018h). *Definition sich verhalten,* Bibliographisches Institut GmbH. Zugriff am 27.10.2018. Verfügbar unter https://www.duden.de/rechtschreibung/verhalten_handeln_sein_reagieren

Duden. (2018i). *Definition Signal,* Bibliographisches Institut GmbH. Zugriff am 27.10.2018. Verfügbar unter https://www.duden.de/rechtschreibung/Signal

Duden. (2018j). *Definition Verhalten,* Bibliographisches Institut GmbH. Zugriff am 27.10.2018. Verfügbar unter http://www.duden.de/rechtschreibung/Verhalten

Duden. (2018k). *Definition Wissen,* Bibliographisches Institut GmbH. Zugriff am 27.10.2018. Verfügbar unter http://www.duden.de/rechtschreibung/Wissen

ECC Köln. (2018). *Anteil von Amazon am Umsatz im Online-Handel in Deutschland nach Plattform in den Jahren 2010 bis 2017.* Zugriff am 29.10.2018. Verfügbar unter https://de.statista.com/statistik/daten/studie/910475/umfrage/anteil-von-amazon-am-umsatz-im-online-handel-nach-plattform-in-deutschland/

Egelman, S., Cranor, L. F. & Hong, J. (2008). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In Proceeding *of the twenty-sixth annual SIGCHI conference on Human factors in computing systems* (S. 1065–1074).

Eid, M., Gollwitzer, M. & Schmitt, M. (2010). *Statistik und Forschungsmethoden. Lehrbuch. Mit Online-Materialien* (Deutsche Erstausgabe). Weinheim, Basel: Beltz Verlagsgruppe.

Endruweit, G. (Hrsg.). (2014). *Wörterbuch der Soziologie* (UTB, Bd. 8566, 3., völlig überarb. Aufl.). Konstanz: UVK-Verl.-Ges; UTB.

English Oxford Dictionaries (Oxford University Press, Hrsg.). (2018). *Definition of knowledge.* Zugriff am 29.05.2017. Verfügbar unter https://en.oxforddictionaries.com/definition/knowledge

Ergoneers GmbH. *Eye Tracking Dikablis Glasses.* Zugriff am 31.10.2018. Verfügbar unter https://www.ergoneers.com/eye-tracking/dikablis-glasses/

Figner, B. & Weber, E. U. (2011). Who Takes Risks When and Why? *Current Directions in Psychological Science, 20* (4), 211–216.

Fishbein, M. & Ajzen, I. (1975). Belief, attitude, intention, and behavior: An introduction to theory and research.

Fishbein, M. & Ajzen, I. (2011). *Predicting and Changing Behavior: The Reasoned Action Approach:* Taylor & Francis.

Fitts, P. M., Jones, R. E. & Milton, J. L. (1950). Eye Movement of Aircraft Pilots during Instrument-Landing Approaches. *Aeronautical Engineering Review* (9), 24–29.

Fogg, B. J., Marshall, J., Laraki, O., Osipovich, A., Varma, C., Fang, N. et al. (2001). What makes Web sites credible?: a report on a large quantitative study. In Proceedings *of the SIGCHI conference on Human factors in computing systems* (S. 61–68).

Forsythe, S., Liu, C., Shannon, D. & Gardner, L. C. (2006). Development of a scale to measure the perceived benefits and risks of online shopping. *Journal of interactive marketing, 20* (2), 55–75.

Forsythe, S. M. & Shi, B. (2003). Consumer patronage and risk perceptions in Internet shopping. *Journal of Business Research, 56* (11), 867–875. Zugriff am 08.09.2015. Verfügbar unter http://www.sciencedirect.com/science/article/pii/S0148296301002739

Foulsham, T. & Underwood, G. (2008). What can saliency models predict about eye movements? Spatial and sequential aspects of fixations during encoding and recognition. *Journal of Vision, 8* (2), 1–17. Zugriff am 08.02.2017. Verfügbar unter http://jov.arvojournals.org/article.aspx?articleid=2158196

Frankenpost Verlag GmbH. (2018). *Fakeshops locken mit Schnäppchen im Internet.* Zugriff am 27.06.2018. Verfügbar unter https://www.frankenpost.de/leben/netzwelt-multimedia/dpa/digitales/berichte/art661183,6069463

Freepik.com, Flaticon (Mitarbeiter). (o.D.). *View eye interface symbol.* Zugriff am 31.10.2018. Verfügbar unter https://www.freepik.com/free-icon/view-eye-interface-symbol_723238.htm

Furby, L. & Beyth-Marom, R. (1992). Risk taking in adolescence: A decision-making perspective. *Developmental Review, 12* (1), 1–44. Zugriff am 24.08.2017. Verfügbar unter http://www.sciencedirect.com/science/article/pii/027322979290002J

Goldberg, J. H., Stimson, M. J., Lewenstein, M., Scott, N. & Wichansky, A. M. (2002). Eye tracking in web search tasks: design implications. In Proceedings *of the 2002 symposium on Eye tracking research & applications* (S. 51–58). ACM. Zugriff am 22.08.2016. Verfügbar unter http://dl.acm.org/citation.cfm?id=507082

Goldstein, E. B. (2008). *Wahrnehmungspsychologie* (7. Aufl.). Berlin Heidelberg: Springer Berlin / Heidelberg.

Goldstein, L., Wagenknecht, E., Schirmer, P. & Wiecha, P. (2013). *Evaluation eines Online-Quiz zur IT-Sicherheits-Expertise*. Tutorium. Technische Universität Darmstadt, Darmstadt.

Gosling, S. D., Vazire, S., Srivastava, S. & John, O. P. (2004). Should we trust web-based studies? A comparative analysis of six preconceptions about internet questionnaires. *American Psychologist, 59* (2), 93. Zugriff am 09.08.2012. Verfügbar unter http://psycnet.apa.org/journals/amp/59/2/93/

Granka, L. A., Joachims, T. & Gay, G. (2004). Eye-tracking analysis of user behavior in WWW search. In Proceedings *of the 27th annual international ACM SIGIR conference on Research and development in information retrieval* (S. 478–479). ACM. Zugriff am 28.06.2016. Verfügbar unter http://dl.acm.org/citation.cfm?id=1009079

Green, P. (2002). Where do drivers look while driving (and for how long). In P. L. Olson & R. E. Dewar (Hrsg.), *Human factors in traffic safety* (2. Aufl., S. 77–110). Lawyers & Judges Pub. Zugriff am 23.03.2017. Verfügbar unter http://apps.usd.edu/coglab/schieber/docs/green2002.pdf

Greenwald, S. J., Olthoff, K. G., Raskin, V. & Ruch, W. (2004). The user non-acceptance paradigm: INFOSEC's dirty little secret. In Proceedings *of the 2004 workshop on New security paradigms* (S. 35–43).

Groeben, N. (1986). *Handeln, Tun, Verhalten als Einheiten einer verstehend-erklärenden Psychologie: wissenschaftstheoretischer Überblick und Programmentwurf zur Integration von Hermeneutik und Empirismus:* Francke.

Hacker, W. (2010). Psychische Regulation von Arbeitstätigkeiten. In N. Birbaumer, D. Frey, J. Kuhl, W. Schneider & R. Schwarzer (Hrsg.), *Enzyklopädie der Psychologie/ Themenbereich D: Praxisgebiete* (Wirtschafts-, Organisations- und Arbeitspsychologie, 1 Arbeitspsychologie, S. 1148). Göttingen: Hogrefe Verlag GmbH & Co KG.

Hanoch, Y., Johnson, J. G. & Wilke, A. (2006). Domain specificity in experimental measures and participant recruitment an application to risk-taking behavior. *Psychological Science, 17* (4), 300–304.

Hardee, J. B., Mayhorn, C. B. & West, R. (2016). I Downloaded What? An Examination of Computer Security Decisions. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 50* (17), 1817–1820. https://doi.org/10.1177/154193120605001721

Hargittai, E. (2005). Survey measures of web-oriented digital literacy. *Social Science Computer Review, 23* (3), 371–379. Zugriff am 16.01.2015. Verfügbar unter http://ssc.sagepub.com/content/23/3/371.short

Hargittai, E. (2007). A framework for studying differences in people's digital media uses. In *Grenzenlose Cyberwelt?* (S. 121–136). Springer. Zugriff am 16.01.2015. Verfügbar unter http://link.springer.com/chapter/10.1007/978-3-531-90519-8_7

Harris, C. R., Jenkins, M. & Glaser, D. (2006). Gender differences in risk assessment: Why do women take fewer risks than men. *Judgment and Decision Making, 1* (1), 48–63.

HDE Handelsverband Deutschland. (2018). *Handel digital. Online-Monitor 2018.* Zugriff am 20180627. Verfügbar unter https://www.einzelhandel.de/index.php?option=com_attachments&task=download&id=9449

Heckhausen, H. (1989). *Motivation und Handeln (2., völlig überarbeitete und ergänzte Auflage)*. Berlin Heidelberg New York: Springer Berlin / Heidelberg.

Heidmann, F. & Ziegler, J. (2002). Web Usability Eye Tracking. *i-com Zeitschrift für interaktive und kooperative Medien, 1* (1/2002), 54.

Heise online, Stefan Krempl (Mitarbeiter). (2012, 18. Oktober). *Verfassungsrichter: "Soviel Datenschutz wie nötig, so wenig wie möglich"*. Zugriff am 07.03.2018. Verfügbar unter https://www.heise.de/newsticker/meldung/Verfassungsrichter-Soviel-Datenschutz-wie-noetig-so-wenig-wie-moeglich-1731923.html

Helmert, J. R., Symmank, C., Pannasch, S. & Rohm, H. (2017). Have an eye on the buckled cucumber. An eye tracking study on visually suboptimal foods. *Food Quality and Preference, 60,* 40–47. https://doi.org/10.1016/J.FOODQUAL.2017.03.009

Helo, A., Pannasch, S., Sirri, L. & Rämä, P. (2014). The maturation of eye movement behavior: Scene viewing characteristics in children and adults. *Vision research, 103,* 83–91. Zugriff am 17.03.2017. Verfügbar unter http://www.sciencedirect.com/science/article/pii/S0042698914001850

Herrmann, D. (2016). Unerfreulich auskunftsfreudig. Inferenzangriffe auf DNS-Anfragen bedrohen unsere Privatsphäre. In Datenbank *Spektrum* (Bd. 16, S. 119–126). https://doi.org/10.1007/s13222-016-0217-6

Hewson, C. M., Laurent, D. & Vogel, C. M. (1996). Proper methodologies for psychological and sociological studies conducted via the Internet. *Behavior Research Methods, 28* (2), 186–191. Zugriff am 09.08.2012. Verfügbar unter http://www.springerlink.com/index/L277J30734336286.pdf

Holmqvist, K., Nyström, M., Andersson, R., Dewhurst, R., Jarodzka, H. & van de Weijer, J. (2011). *Eye tracking: A comprehensive guide to methods and measures:* OUP Oxford.

Huber, O. (2005). *Das psychologische Experiment* (4. Aufl.). Bern, CH: Huber.

Huey, E. B. (1898). Preliminary experiments in the physiology and psychology of reading. *The American Journal of Psychology, 9* (4), 575–586. Zugriff am 07.07.2016. Verfügbar unter http://www.jstor.org/stable/1412192

Institut für angewandte Sozialwissenschaften. (2014). *Millionendelikt Internetbetrug*. Bonn. Zugriff am 10.08.2018. Verfügbar unter https://www.infas.de/fileadmin/user_upload/PDF/infas_PM_Millionendelikt_Internetbetrug_20140711.pdf

Initiative D21. (2018). *Anteil der Internetnutzer in Deutschland in den Jahren 2001 bis 2017* (D21-Digital-Index 2017/2018). Zugriff am 07.03.2018. Verfügbar unter https://de.statista.com/statistik/daten/studie/13070/umfrage/entwicklung-der-internetnutzung-in-deutschland-seit-2001/

Jacob, R. J. & Karn, K. S. (2003). Eye tracking in human-computer interaction and usability research: Ready to deliver the promises. *Mind, 2* (3), 4. Zugriff am 21.08.2016. Verfügbar unter http://www.academia.edu/download/4589771/10.1.1.100.445.pdf

Jacob, R. J. K. (1990). What you look at is what you get: eye movement-based interaction techniques. In Proceedings *of the SIGCHI conference on Human factors in computing systems* (S. 11–18). ACM. Zugriff am 18.03.2017. Verfügbar unter http://dl.acm.org/citation.cfm?id=97246

Jiuan Tan, S. (1999). Strategies for reducing consumers' risk aversion in Internet shopping. *Journal of Consumer Marketing, 16* (2), 163–180. https://doi.org/10.1108/07363769910260515

Johnson, J. G., Wilke, A. & Weber, E. U. (2004). Beyond a trait view of risk taking: A domain-specific scale measuring risk perceptions, expected benefits, and perceived-risk attitudes in German-speaking populations. *Polish Psychological Bulletin, 35* (3), 153–164.

Kahneman, D. & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica, 47* (2), 263–292. https://doi.org/10.2307/1914185

Kim, H.-W., Xu, Y. & Gupta, S. (2012). Which is more important in Internet shopping, perceived price or trust? *Electronic Commerce Research and Applications, 11* (3), 241–252. https://doi.org/10.1016/j.elerap.2011.06.003

Kleiner Perkins Caufield & Byers, CB Insights, Wall Street Journal & S&P Capital IQ. (05/2017). *Internet Trends 2017* (Kleiner Perkins Caufield & Byers, Hrsg.). Zugriff am 08.03.2018. Verfügbar unter https://de.statista.com/statistik/daten/studie/187086/umfrage/internetunternehmen-nach-ihrem-umsatz-weltweit/

Köcher, R. (2015). *Schöne neue Welt. Das Internet erleichtert vieles. Es wird kräftig genutzt. Bei vielen regt sich aber auch Skepsis über mögliche Folgen der Vernetzung* (Frankfurter Allgemeine Zeitung, Hrsg.). Institut für Demoskopie Allensbach. Zugriff am 08.03.2018. Verfügbar unter https://www.ifd-allensbach.de/uploads/tx_reportsndocs/FAZ_April_Digitalisierung.pdf

Kraut, R., Olson, J., Banaji, M., Bruckman, A., Cohen, J. & Couper, M. (2004). Psychological research online: report of Board of Scientific Affairs' Advisory Group on the Conduct of Research on the Internet. *American Psychologist, 59* (2), 105. Zugriff am 09.08.2012. Verfügbar unter http://psycnet.apa.org/journals/amp/59/2/105/

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J. & Nunge, E. (2007). Protecting people from phishing: the design and evaluation of an embedded training email system. In Proceedings *of the SIGCHI conference on Human factors in computing systems* (S. 905–914).

Kumaraguru, P., Acquisti, A. & Cranor, L. F. (2006). Trust modelling for online transactions. A phishing Scenario. https://doi.org/10.1145/1501434.1501448

Lackes, R., Siepermann, M. & Kollmann, T. (Gabler Verlag, Hrsg.). (2018). *Gabler Wirtschaftslexikon - Electronic Shopping/ Onlineshopping,* Springer Fachmedien Wiesbaden GmbH. Zugriff am 27.10.2018. Verfügbar unter http://wirtschaftslexikon.gabler.de/Archiv/76283/electronic-shopping-v12.html

LaRose, R., Rifon, N. J. & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM, 51* (3), 71–76. https://doi.org/10.1145/1325555.1325569

Laux, H. (Hrsg.). (2005). *Entscheidungstheorie* (Springer-Lehrbuch, 6., durchges. Aufl.). Berlin: Springer Berlin Heidelberg; Springer.

Leonhart, R. & Maurischat, C. (2004). Meta-Analysen auf Primärdatenbasis - Probleme und Lösungsansätze. *Zeitschrift für Evaluation* (1), 21–34.

Linguee Wörterbuch. (2018). *Wörterbuch Englisch-Deutsch*. Übersetzung "cue", DeepL GmbH. Zugriff am 27.10.2018. Verfügbar unter https://www.linguee.de/deutsch-englisch/search?source=auto&query=cue

Loftus, G. R. & Mackworth, N. H. (1978). Cognitive determinants of fixation location during picture viewing. *Journal of Experimental Psychology: Human Perception and Performance, 4* (4), 565–572. https://doi.org/10.1037/0096-1523.4.4.565

MageReport. (o.D.). *Scan your Magento shop now for known vulnerabilities.* Zugriff am 31.08.2018. Verfügbar unter https://www.magereport.com/

Magin, J. (2013). *Einfluss von Internetsicherheit-Expertise auf Risikoverhalten im Internet*. Bachelorthesis. Technische Universität Darmstadt, Darmstadt.

Mann, H. B. & Whitney, D. R. (1947). On a Test of Whether one of Two Random Variables is Stochastically Larger than the Other. *The Annals of Mathematical Statistics* (18), 50–60. Zugriff am 03.11.2018. Verfügbar unter https://www.jstor.org/stable/pdf/2236101.pdf

McDonald, A. & Cranor, L. F. (2010). Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising. *TPRC 2010.* Zugriff am 08.03.2018. Verfügbar unter https://ssrn.com/abstract=1989092

Miyazaki, A. D. & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer affairs, 35* (1), 27–44. Zugriff am 24.02.2017. Verfügbar unter http://onlinelibrary.wiley.com/doi/10.1111/j.1745-6606.2001.tb00101.x/full

Moosbrugger, H. & Kelava, A. (2007). *Testtheorie und Fragebogenkonstruktion:* Springer.

Muthén, L. K. & Muthén, B. O. (2002). How to use a Monte Carlo study to decide on sample size and determine power. *Structural Equation Modeling, 9* (4), 599–620.

Myers, R. H. (1990). *Classical and modern regression with applications* (Duxbury classic series, 2. Aufl.). Pacific Grove, CA: Duxbury/Thompson Learning.

Netcraft LTD. (2018). *Netcraft Extension.* Zugriff am 31.08.2018. Verfügbar unter https://toolbar.netcraft.com/

Norberg, P. A., Horne, D. R. & Horne, D. A. (2007). The Privacy Paradox. Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer affairs, 41* (1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Norddeutscher Rundfunk. (2016). *Nackt im Netz: Millionen Nutzer ausgespäht.* Zugriff am 31.10.2018. Verfügbar unter https://www.ndr.de/nachrichten/netzwelt/Nackt-im-Netz-Millionen-Nutzer-ausgespaeht,nacktimnetz100.html

Novak, T. P., Hoffman, D. L. & Yung, Y. F. (2000). Measuring the customer experience in online environments: A structural modeling approach. *Marketing Science, 19* (1), 22–42. Zugriff am 05.12.2012. Verfügbar unter http://marketsci.highwire.org/content/19/1/22.short

Oehme, A. & Jürgensohn, T. (2006). Arbeitskreis Blickbewegung: Chancen und Schwächen der Blickanalyse bei der Bewertung von Objekten. *MMI-Interaktiv Ausgabe August 2006,* 3. Zugriff am 07.07.2016. Verfügbar unter https://www.researchgate.net/profile/Jeronimo_Dzaack/publication/26439739_Kognitive_Modellierung_in_dynamischen_Mensch-Maschine-Systemen/links/0deec5273b493af636000000.pdf#page=7

Olejnik, L., Castelluccia, C. & Janc, A. (2014). On the uniqueness of Web browsing history patterns. *annals of telecommunications - annales des télécommunications, 69* (1-2), 63–74. https://doi.org/10.1007/s12243-013-0392-5

Olivero, N. & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges. The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology, 25* (2), 243–262. https://doi.org/10.1016/S0167-4870(02)00172-1

Ollermann, F. (2004). Verhaltensbasierte Validierung von Usability-Fragebögen. In Mensch & *Computer* (S. 55–64).

Page, K., Robson, M. & Uncles, M. D. (2012). Perceptions of Web Knowledge and Usability: When Sex and Experience Matter. *International journal of human-computer studies.* Zugriff am 05.12.2012. Verfügbar unter http://www.sciencedirect.com/science/article/pii/S1071581912001292

Page, K. & Uncles, M. (2004). Consumer knowledge of the World Wide Web: Conceptualization and measurement. *Psychology and Marketing, 21* (8), 573–591.

Pan, B., Hembrooke, H. A., Gay, G. K., Granka, L. A., Feusner, M. K. & Newman, J. K. (2004). The determinants of web page viewing behavior: an eye-tracking study. In Proceedings *of the 2004 symposium on Eye tracking research & applications* (S. 147–154). San Antonio, Texas: ACM. Zugriff am 14.03.2017. Verfügbar unter http://dl.acm.org/citation.cfm?id=968391

Park, C.-H. & Kim, Y.-G. (2003). Identifying key factors affecting consumer purchase behavior in an online shopping context. *International journal of retail & distribution management, 31* (1), 16–29. https://doi.org/10.1108/09590550310457818

Pfeiffer, T., Theuerling, H. & Kauer, M. (2013). Click Me If You Can! In Human *Aspects of Information Security, Privacy, and Trust* (S. 155–166). Springer. Zugriff am 15.08.2013. Verfügbar unter http://link.springer.com/chapter/10.1007/978-3-642-39345-7_17

Pillai, K. G. & Hofacker, C. (2007). Calibration of consumer knowledge of the web. *International Journal of Research in Marketing, 24* (3), 254–267. Zugriff am 15.01.2015. Verfügbar unter http://www.sciencedirect.com/science/article/pii/S0167811607000304

Polizei Niedersachsen. (o.D.). *Ratgeber Internetkriminaliät. Onlineshopping und Betrug.* Zugriff am 18.04.2018. Verfügbar unter https://www.polizei-praevention.de/themen-und-tipps/onlineshopping.html

Pommerening, K. (1991). *Datenschutz und Datensicherheit:* BI-Wiss.-Verlag.

Pommerening, K. (2004). *Grundprobleme von Datenschutz und Datensicherheit. Grundbegriffe*. Verfügbar unter http://klauspommerening.de/DSVorlesung/Grundprobleme/Begriffe.html

Poole, A. & Ball, L. J. (2006). Eye tracking in HCI and usability research. *Encyclopedia of human computer interaction, 1,* 211–219.

Potosky, D. (2007). The Internet knowledge (iKnow) measure. *Computers in Human behavior, 23* (6), 2760–2777. Zugriff am 05.12.2012. Verfügbar unter http://www.sciencedirect.com/science/article/pii/S0747563206000732

Raju, P. S., Lonial, S. C. & Mangold, W. G. (1995). Differential effects of subjective knowledge, objective knowledge, and usage experience on decision making: An exploratory investigation. *Journal of consumer psychology, 4* (2), 153–180. Zugriff am 31.05.2017. Verfügbar unter http://www.sciencedirect.com/science/article/pii/S1057740895704284

Raman, P. & Pashupati, K. (2004). Online privacy: the impact of self perceived technological competence, *15,* 5–6.

Rayner, K. (1978). Eye movement latencies for parafoveally presented words. *Bulletin of the Psychonomic Society, 11* (1), 13–16. https://doi.org/10.3758/BF03336753

Rayner, K. (1998). Eye movements in reading and information processing: 20 years of research. *Psychological bulletin, 124* (3), 372. Zugriff am 16.03.2017. Verfügbar unter http://psycnet.apa.org/journals/bul/124/3/372/

Razali, N. M. & Wah, Y. B. (2011). Power comparisons of shapiro-wilk, kolmogorov-smirnov, lilliefors and anderson-darling tests. *Journal of statistical modeling and analytics, 2* (1), 21–33.

Rhee, H.-S., Ryu, Y. & Kim, C.-T. (2005). I am fine but you are not: Optimistic Bias and Illusion of Control on Information Security. *Proceedings of the International Conference on Information Systems (ICIS),* 381–394. Zugriff am 29.10.2018. Verfügbar unter https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1238&context=icis2005

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of psychology, 91* (1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Ross, C., Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G. & Orr, R. R. (2009). Personality and motivations associated with Facebook use. *Computers in Human behavior, 25* (2), 578–586. https://doi.org/10.1016/j.chb.2008.12.024

Roßnagel, A., Geminn, C. L., Jandt, S. & Richter, P. (Hrsg.). (2016). *Datenschutzrecht 2016 - "smart" genug für die Zukunft? Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts* (ITeG - Interdisciplinary Research on Information System Design, Band 4). Kassel: Kassel University Press. https://doi.org/10.19211/KUP9783737601559

Rudolf, M. & Müller, J. (2011). *Multivariate Verfahren. Eine praxisorientierte Einführung mit Anwendungsbeispielen in SPSS* (2. Aufl.). Göttingen: Hogrefe.

Salvucci, D. D. & Goldberg, J. H. (2000). Identifying fixations and saccades in eye-tracking protocols. In Proceedings *of the 2000 symposium on Eye tracking research & applications* (S. 71–78). ACM. Zugriff am 28.06.2016. Verfügbar unter http://dl.acm.org/citation.cfm?id=355028

Schechter, S. E., Dhamija, R., Ozment, A. & Fischer, I. (2007). The emperor's new security indicators. In Security *and Privacy, 2007. SP'07. IEEE Symposium on* (S. 51–65).

Schlick, C., Bruder, R. & Luczak, H. (2018). *Arbeitswissenschaft* (4. Auflage). Berlin: Springer Vieweg. https://doi.org/10.1007/978-3-662-56037-2

Schoemaker, P. (1990). Are risk-attitudes related across domains and response modes? *Management science,* 1451–1463.

Sibert, L. E. & Jacob, R. J. K. (2000). Evaluation of eye gaze interaction. In Proceedings *of the SIGCHI conference on Human Factors in Computing Systems* (S. 281–288). ACM. Zugriff am 22.02.2017. Verfügbar unter http://dl.acm.org/citation.cfm?id=332445

SINUS-Institut Heidelberg. (2012). *DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet*. Hamburg.

Sitkin, S. B. & Pablo, A. L. (1992). Reconceptualizing the determinants of risk behavior. *Academy of management review,* 9–38. Zugriff am 18.07.2012. Verfügbar unter http://www.jstor.org/stable/10.2307/258646

Smith, H. J., Milberg, S. J. & Burke, S. J. (1996). Information Privacy. Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly, 20* (2), 167–196. https://doi.org/10.2307/249477

(o.D.). SoSciSurvey.de [Computer software]: SoSci Survey GmbH. Verfügbar unter https://www.soscisurvey.de/

DIN EN ISO 15007-1: 2015-03. *Straßenfahrzeuge - Messung des Blickverhaltens von Fahrern bei Fahrzeugen mit Fahrerinformations- und -assistenzsystemen - Teil 1: Begriffe und Parameter (ISO 15007-1:2014):* Beuth Verlag GmbH.

Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N. & Cranor, L. F. (2009). Crying wolf: An empirical study of SSL warning effectiveness. In Proceedings *of the 18th conference on USENIX security symposium* (S. 399–416).

Sweeney, J. C., Soutar, G. N. & Johnson, L. W. (1999). The role of perceived risk in the quality-value relationship. A study in a retail environment. *Journal of Retailing, 75* (1), 77–105. https://doi.org/10.1016/S0022-4359(99)80005-0

Tatler, B. W. (2007). The central fixation bias in scene viewing: Selecting an optimal viewing position independently of motor biases and image feature distributions. *Journal of Vision, 7* (14), 4. Zugriff am 08.02.2017. Verfügbar unter http://jov.arvojournals.org/article.aspx?articleid=2122066

Taylor, P., He, Z., Bilgrien, N. & Siegelmann, H. T. (2015). Human strategies for multitasking, search, and control improved via real-time memory aid for gaze location. *Frontiers in ICT, 2,* 15.

The Solid Project. (o.D.). Verfügbar unter https://solid.mit.edu/

Tinker, M. A. (1958). Recent studies of eye movements in reading. *Psychological bulletin, 55* (4), 215–231. https://doi.org/10.1037/h0041228

Trusted Shops GmbH, Mustafa Uçar (Mitarbeiter). (2016). *Checklist: So erkennst du gefälschte Online Shops Checkliste: So erkennst Du gefälschte Online Shops.* Zugriff am 13.03.2018. Verfügbar unter https://www.trustedshops.de/blog/gefaelschte-online-shops/

Tsai, J. Y., Egelman, S., Cranor, L. & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22* (2), 254–268.

Tsow, A. & Jakobsson, M. (2007). *Deceit and deception: A large user study of phishing*.

Urbany, J. E., Dickson, P. R. & Wilkie, W. L. (1989). Buyer Uncertainty and Information Search. *Journal of Consumer Research, 16* (2), 208. https://doi.org/10.1086/209209

Van Deursen, A. & van Dijk, J. (2010). Measuring internet skills. *Intl. Journal of Human–Computer Interaction, 26* (10), 891–916.

Van Dijk, J. & van Deursen, A. (2010). Traditional media skills and digital media skills: Much of a difference. In ICA *conference.* Zugriff am 23.01.2015. Verfügbar unter http://www.alexandervandeursen.nl/Joomla/Articles/Conference/2010_TradDigital_DeursenDijk.pdf

Velichkovsky, B. M., Dornhoefer, S. M., Pannasch, S. & Unema, P. J. A. (2000). Visual fixations and level of attentional processing. In Proceedings *of the 2000 symposium on Eye tracking research & applications* (S. 79–85). ACM. Zugriff am 16.03.2017. Verfügbar unter http://dl.acm.org/citation.cfm?id=355029

Velichkovsky, B. M., Joos, M., Helmert, J. R. & Pannasch, S. (2005). Two visual systems and their eye movements: Evidence from static and dynamic scene perception. In Proceedings *of the XXVII conference of the cognitive science society* (S. 2283–2288). Citeseer. Zugriff am 14.09.2016. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.486.9238&rep=rep1&type=pdf

Velichkovsky, B. M., Sprenger, A. & Pomplun, M. (1997). *Auf dem Weg zur Blickmaus: Die Beeinflussung der Fixationsdauer durch kognitive und kommunikative Aufgaben* (Software-Ergonomie '97. Berichte des German Chapter of the ACM, Bd. 49): Vieweg+Teubner Verlag.

Wade, N. & Tatler, B. W. (2005). *The moving tablet of the eye: The origins of modern eye movement research:* Oxford University Press, USA.

Waldman, A. E. (2018). *Privacy, Notice, and Design*. Stanford Technology Law Review. Stanford Law School, Stanford, California. Zugriff am 20181027. Verfügbar unter https://www-cdn.law.stanford.edu/wp-content/uploads/2018/01/Waldman_FINAL-Formatted-011818.pdf

Wambach, T. (2017). Ökonomisierung von Nutzerverhalten – historische Entwicklung und aktueller Stand. *Forschungsjournal Soziale Bewegungen, 30* (2), 162–169. https://doi.org/10.1515/fjsb-2017-0037

Wambach, T. & Bräunlich, K. (2017). The Evolution of Third-Party Web Tracking. In Information *Systems Security and Privacy; ICISSP 2016; Communications in Computer and Information Science* (Bd. 691).

Wambach, T. & Bräunlich, K. (2016). Retrospective Study of Third-party Web Tracking. *Proceedings of the 2nd International Conference on Information Systems Security and Privacy : Rome, Italy, February 19-21,* 138–145. https://doi.org/10.5220/0005741301380145

Wang, S., Beatty, S. E. & Foxx, W. (2004). Signaling the trustworthiness of small online retailers. *Journal of interactive marketing, 18* (1), 53–69. Zugriff am 06.02.2017. Verfügbar unter http://www.sciencedirect.com/science/article/pii/S1094996804700973

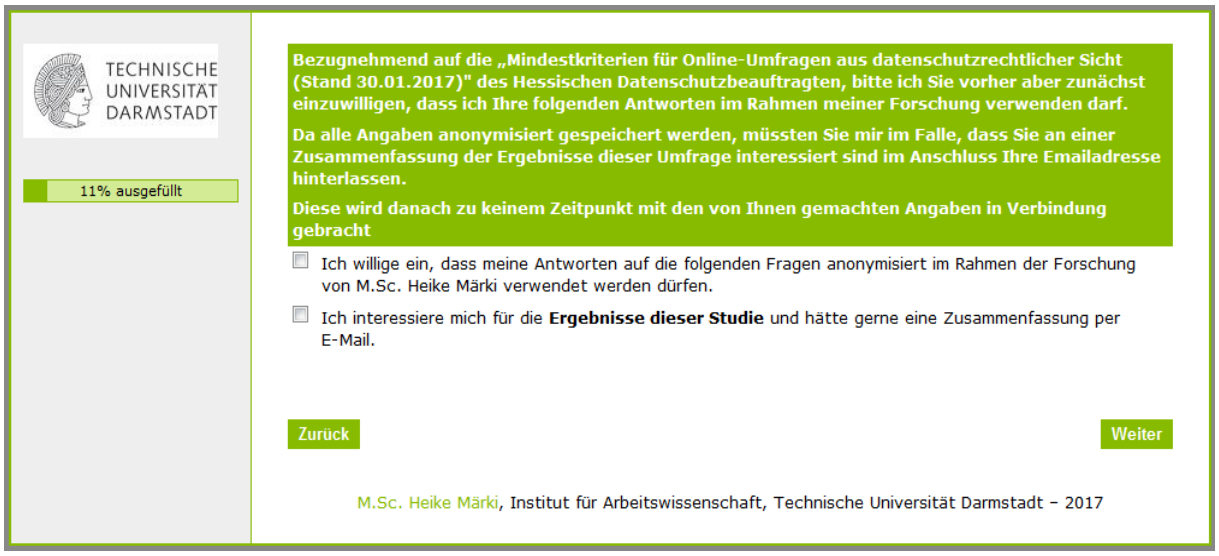
Weber, E. U. (1997). The utility of measuring and modeling perceived risk. *Choice, decision, and measurement: Essays in honor of R. Duncan Luce,* 45–57.
Weber, E. U., Blais, A. R. & Betz, N. E. (2002). A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. *Journal of behavioral decision making, 15* (4), 263–290.
Weber, E. U. & Hsee, C. (1998). Cross-cultural differences in risk perception, but cross-cultural similarities in attitudes towards perceived risk. *Management science,* 1205–1217.
Weber, M. (2002). *Wirtschaft und Gesellschaft: Grundriß der Verstehenden Soziologie* (Nachdruck der 5. Auflage). Tübingen: Mohr Siebeck.
Weiber, R. & Mühlhaus, D. (2014). *Strukturgleichungsmodellierung. Eine anwendungsorientierte Einführung in die Kausalanalyse mit Hilfe von AMOS, SmartPLS und SPSS* (Springer-Lehrbuch, 2., erw. und korr. Aufl.). Berlin, Heidelberg: Springer Berlin Heidelberg; Springer Gabler. https://doi.org/10.1007/978-3-642-35012-2
West, R. (2008). The psychology of security. *Communications of the ACM, 51* (4), 34–40.
Whalen, T. & Inkpen, K. M. (2005). Gathering evidence: use of visual security cues in web browsers. In Proceedings *of Graphics Interface 2005* (S. 137–144).
Wild, E. & Möller, J. (Hrsg.). (2009). *Pädagogische Psychologie. Wissenserwerb*. Heidelberg: Springer Medizin Verlag.
Wilke, A., Hutchinson, J. M. C., Todd, P. M. & Kruger, D. J. (2006). Is Risk Taking Used as a Cue in Mate Choice? *Evolutionary Psychology, 4* (1). https://doi.org/10.1177/147470490600400130
Wirtz, M. A. (Hrsg.). (2014). *Risikowahl-Modell* (Dorsch -Lexikon der Psychologie, 18. Aufl.). Bern: Hogrefe Verlag.
Wu, M., Miller, R. C. & Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? In Proceedings *of the SIGCHI conference on Human Factors in computing systems* (S. 601–610).
Ye, Z., Smith, S. & Anthony, D. (2005). Trusted paths for browsers. *ACM Transactions on Information and System Security, 8* (2), 153–186. https://doi.org/10.1145/1065545.1065546
Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents // Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *Journal of Consumer affairs, 43* (3), 389–418. https://doi.org/10.1111/j.1745-6606.2009.01146.x
Zimbardo, P. G. & Gerrig, R. J. (2003). *Psychologie* (Springer-Lehrbuch, 7., neu übers. und bearb. Aufl., Nachdr). Berlin: Springer.
Zimmermann, U. (2014). Fixationsdauer - wichtige Messgrösse für Usability & Marketing Analysen. *Eye Tracking Kompetenzzentrum Schweiz.* Zugriff am 22.03.2017. Verfügbar unter http://eyetracking.ch/glossar-fixationsdauer/

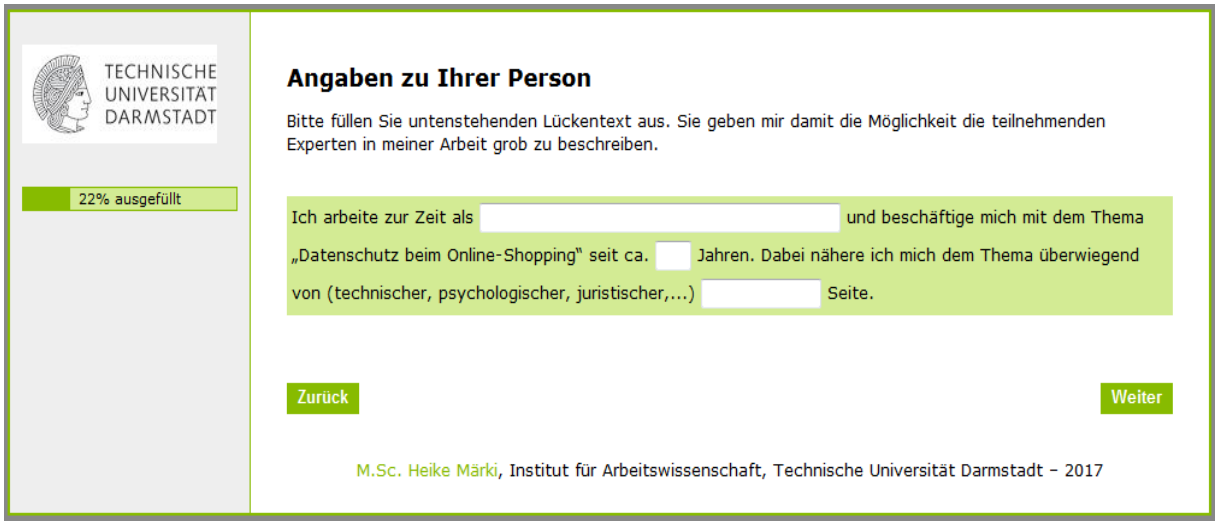
Anhangsverzeichnis

Anhang A - Fragebogen der Gewichtungsstudie
Anhang B - Fragebogen der Explorations- bzw. Validierungsstudie
Anhang C - Einverständniserklärung und Instruktion
Anhang D - In Explorationsstudie untersuchte Hypothesen
Anhang E - SPSS Ausgabe der Modellberechnungen zu Modell 1
Anhang F - SPSS Ausgabe der Modellberechnungen zu Modell 2

Anhang A

Fragebogen der Gewichtungsstudie





TECHNISCHE UNIVERSITÄT DARMSTADT

33% ausgefüllt

Im Weiteren gehen wir von folgendem Szenario aus:

Ein Nutzer möchte auf der Webseite eines ihm/ihr bislang unbekannten Webshops ein Produkt kaufen.

Welche Inhalte der Webseite können ihm/ihr dabei Aufschluss über den Umgang des Anbieters mit personenbezogenen Daten geben?
Und, wie intensiv muss er/sie sich mit diesem Inhalt auseinandersetzen?
Reicht ein kurzer Blick oder muss ein wenig mehr Zeit investiert werden?

Zurück Weiter

M.Sc. Heike Märki, Institut für Arbeitswissenschaft, Technische Universität Darmstadt – 2017

TECHNISCHE UNIVERSITÄT DARMSTADT

44% ausgefüllt

Wie wichtig ist für jeden der folgenden Inhalte eine kurze Überprüfung des Vorhandenseins mittels eines kurzen Blickes (symbolisiert anhand des Auge-Symbols)?

Und

Wie wichtig ist es für jeden der folgenden Inhalte, sich darüber hinaus eingehender mit diesem zu beschäftigen (symbolisiert anhand des Symbols der Leselupe)?

Bitte schieben Sie BEIDE Symbole jeweils an die Stelle der Skala, die die jeweilige Wichtigkeit repräsentiert. Halten Sie einen der Inhalte für völlig unwichtig, können Sie diesen gerne überspringen und den nächsten wichtigen Inhalt bewerten.

Individuelle Accounts/ Benutzer Log-Ins	unwichtig	wichtig
Klare Preisangabe	unwichtig	wichtig
Angaben zu Widerrufsrecht	unwichtig	wichtig
Sprachoptionen	unwichtig	wichtig
Unterschiedliche Bestellmethoden (Online, Fax, Mail, Telefon...)	unwichtig	wichtig
Veröffentlichungen von Expertenbeurteilungen, unabhängigen Testberichten, Preisen und Awards	unwichtig	wichtig
Verschiedene Versandoptionen	unwichtig	wichtig
Gewerberegister und -nummer	unwichtig	wichtig
Produktempfehlungen	unwichtig	wichtig
Garantien (Produktgarantie, Geld-Zurück-Garantie, Preisgarantie)	unwichtig	wichtig
Shopname (URL)	unwichtig	wichtig
Kundenbeurteilungen des Shops	unwichtig	wichtig
Informationen zum Datenschutz, bzw. Datensicherheit	unwichtig	wichtig
https in URL	unwichtig	wichtig
Informationen zur schnellen Kontaktaufnahme (Telefonnummer, Email, Fax...)	unwichtig	wichtig
Links zu verwandten Websites, bzw. strategischen Partnern	unwichtig	wichtig


Links zu verwandten Websites, bzw. strategischen Partnern
unwichtig
wichtig
Internetbezahlsysteme (z.B. Paypal)
unwichtig
wichtig
Angaben zu Rücksendekosten
unwichtig
wichtig
Gütesiegel
unwichtig
wichtig
Social Bookmarks
unwichtig
wichtig
Umsatzsteuer-Identifikationsnummer
unwichtig
wichtig
Unternehmensname und Rechtsformzusatz
unwichtig
wichtig
Transparenter Bestellvorgang (Bestellfortschrittsanzeige und/oder Gesamtbestellwertanzeige inkl. aller Zusatzkosten)
unwichtig
wichtig
Besucherzähler
unwichtig
wichtig
Firmeninformationen (Wir über uns)
unwichtig
wichtig
Hinweis bezüglich Mehrwertsteuer, bzw. Umsatzsteuer
unwichtig
wichtig
Großes Artikelsortiment
unwichtig
wichtig
FAQ bzw. Hilfesektion
unwichtig
wichtig
Viele Zahlungsmethoden
unwichtig
wichtig
RSS-Feed
unwichtig
wichtig
Hinweis auf Rückgaberechte
unwichtig
wichtig
Verfügbarkeitsanzeige
unwichtig
wichtig
EV-SSL-Zertifikat
unwichtig
wichtig
Produktbeschreibung
unwichtig
wichtig
Auftragsstatusanzeige bzw. Sendungsverfolgung
unwichtig
wichtig
Look-in-Feature (z.B. Bedienungsanleitungseinsicht)
unwichtig
wichtig
Bonusprogramm (z.B. Payback)
unwichtig
wichtig
Allgemeine Geschäftsbedingungen
unwichtig
wichtig
Name und Anschrift des Anbieters
unwichtig
wichtig
Angaben zu Versandkosten
unwichtig
wichtig
Produktbild
unwichtig
wichtig
Zurück
Weiter
M.Sc. Heike Märki, Institut für Arbeitswissenschaft, Technische Universität Darmstadt – 2017

TECHNISCHE UNIVERSITÄT DARMSTADT

67% ausgefüllt

Welches sind in Ihren Augen die wichtigsten Hinweise für den Nutzer einer ihm unbekannten Webseite?

Ziehen Sie diese der Reihe nach (1 = wichtigster Hinweis, 2 = zweitwichtigster Hinweis usw.) in die nummerierten Kästen auf der rechten Seite oder wählen Sie sie der Reihe nach mit einem Doppelklick aus.

Verfügbarkeits-anzeige	Produkt-empfehlungen	Angaben zu Widerrufsrecht
Informationen zu Datenschutz/ Datensicherheit	USt-IdNr.	Experten-beurteilungen, Testberichte...
Produkt-beschreibung	Produktbild	Gewerberegister & -nr.
Social Bookmarks	AGB	Unternehmensname & Rechtsformzusatz
Besucherzähler	Transparenter Bestellvorgang	https in URL
Hinweis auf Rückgaberechte	Kundenbeurteilungen des Shops	Name & Anschrift des Anbieters
Angaben zu Versandkosten	Individuelle Accounts/ Benutzer Log-Ins	Bonusprogramm (z.B. Payback)
Garantien (Produkt-, Geld-Zurück-, Preis-)	Klare Preisangabe	Auftragsstatus-anzeige bzw. Sendungsverfolgung
Viele Zahlungsmethoden	RSS-Feed	Look-in-Feature
Verschiedene Versandoptionen	Gütesiegel	Internet-bezahlsysteme (z.B. Paypal)
Links zu verwandten Websites	FAQ bzw. Hilfesektion	Firmeninformationen (Wir über uns)
Unterschiedliche Bestellmethoden	Großes Artikelsortiment	Shopname (URL)
Informationen zur schnellen Kontaktaufnahme	Angaben zu Rücksendekosten	

1

2

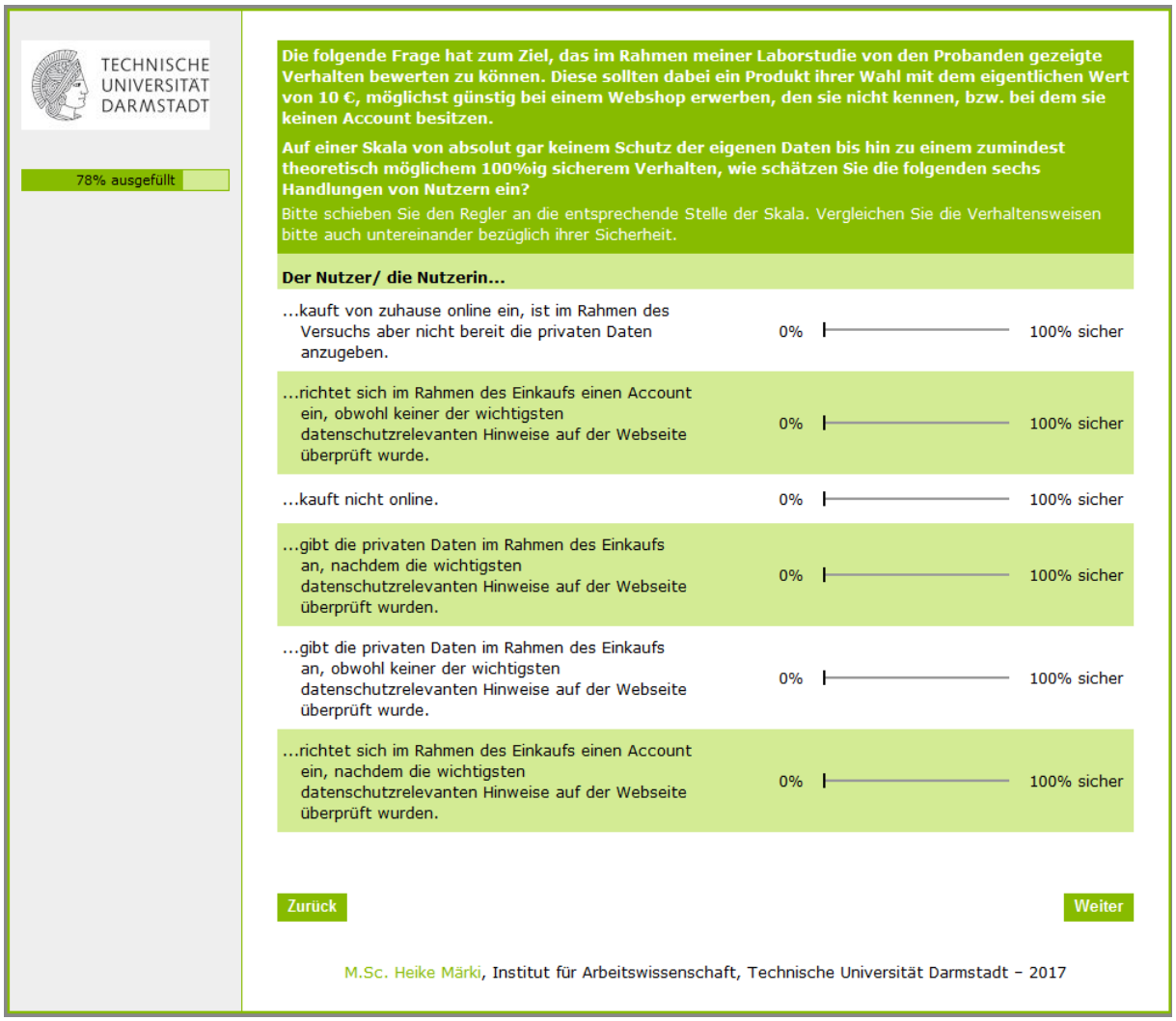
3

4

5

Zurück

Weiter


TECHNISCHE UNIVERSITÄT DARMSTADT
78% ausgefüllt
Die folgende Frage hat zum Ziel, das im Rahmen meiner Laborstudie von den Probanden gezeigte Verhalten bewerten zu können. Diese sollten dabei ein Produkt ihrer Wahl mit dem eigentlichen Wert von 10 €, möglichst günstig bei einem Webshop erwerben, den sie nicht kennen, bzw. bei dem sie keinen Account besitzen.
Auf einer Skala von absolut gar keinem Schutz der eigenen Daten bis hin zu einem zumindest theoretisch möglichem 100%ig sicherem Verhalten, wie schätzen Sie die folgenden sechs Handlungen von Nutzern ein?
Bitte schieben Sie den Regler an die entsprechende Stelle der Skala. Vergleichen Sie die Verhaltensweisen bitte auch untereinander bezüglich ihrer Sicherheit.
Der Nutzer/ die Nutzerin...
...kauft von zuhause online ein, ist im Rahmen des Versuchs aber nicht bereit die privaten Daten anzugeben.
0%
100% sicher
...richtet sich im Rahmen des Einkaufs einen Account ein, obwohl keiner der wichtigsten datenschutzrelevanten Hinweise auf der Webseite überprüft wurde.
0%
100% sicher
...kauft nicht online.
0%
100% sicher
...gibt die privaten Daten im Rahmen des Einkaufs an, nachdem die wichtigsten datenschutzrelevanten Hinweise auf der Webseite überprüft wurden.
0%
100% sicher
...gibt die privaten Daten im Rahmen des Einkaufs an, obwohl keiner der wichtigsten datenschutzrelevanten Hinweise auf der Webseite überprüft wurde.
0%
100% sicher
...richtet sich im Rahmen des Einkaufs einen Account ein, nachdem die wichtigsten datenschutzrelevanten Hinweise auf der Webseite überprüft wurden.
0%
100% sicher
Zurück
Weiter
M.Sc. Heike Märki, Institut für Arbeitswissenschaft, Technische Universität Darmstadt – 2017


TECHNISCHE UNIVERSITÄT DARMSTADT
89% ausgefüllt
Vielen Dank für die Teilnahme an meiner Expertenbefragung!
Diese wird voraussichtlich am 30. Juni 2017 beendet sein.
Falls Sie möchten, können Sie mir im untenstehenden Feld sehr gerne eine Rückmeldung zur Befragung oder auch Inhalt und Vorgehen meiner Dissertation geben.
In jedem Fall bedanke ich mich für Ihre Mithilfe und wünsche Ihnen noch einen schönen Tag,
mit freundlichen Grüßen,
M. Sc. Heike Märki
Bitte klicken Sie noch einmal auf WEITER, danach können Sie das Browser-Fenster schließen.
Zurück
Weiter
M.Sc. Heike Märki, Institut für Arbeitswissenschaft, Technische Universität Darmstadt – 2017

Fragebogen der Explorations- bzw. Validierungsstudie
Teil 1 (vor Bearbeitung der Aufgabe)

0% ausgefüllt

1. In welchem Jahr sind Sie geboren?

Geburtsjahr:

Sie sind ...

- weiblich
- männlich

2. Welchen Bildungsabschluss haben Sie?

Bitte wählen Sie den höchsten Bildungsabschluss, den Sie bisher erreicht haben.

- Noch Schüler
- Schule beendet ohne Abschluss
- Volks-, Hauptschulabschluss
- Mittlere Reife, Realschul- oder gleichwertiger Abschluss
- Abgeschlossene Lehre
- Fachabitur, Fachhochschulreife
- Abitur, Hochschulreife
- Fachhochschul-/Hochschulabschluss
- Anderer Abschluss, und zwar:

3. Wie hoch ist ungefähr Ihr monatliches Haushalts-Nettoeinkommen?

Gemeint ist der Betrag, der sich aus allen Einkünften der Bewohner Ihres Haushalts zusammensetzt und nach Abzug der Steuern und Sozialversicherungen übrig bleibt.

[Bitte auswählen]

Weiter

Institut für Arbeitswissenschaft, Technische Universität Darmstadt

soSci
oFb - der onlineFragebogen

11% ausgefüllt

4. Wie häufig nutzen Sie persönlich das Internet?

Ich nutze das Internet...

- ◯ täglich
- ◯ mehrmals pro Woche
- ◯ ein paar Mal pro Monat
- ◯ seltener

5. Seit wann benutzen Sie bereits das Internet?

Ich benutze das Internet seit...

- ◯ weniger als 3 Jahren
- ◯ 3 bis unter 7 Jahren
- ◯ 7 bis unter 10 Jahren
- ◯ mehr als 10 Jahren

6. Welche Geräte besitzen Sie?

Ich besitze...

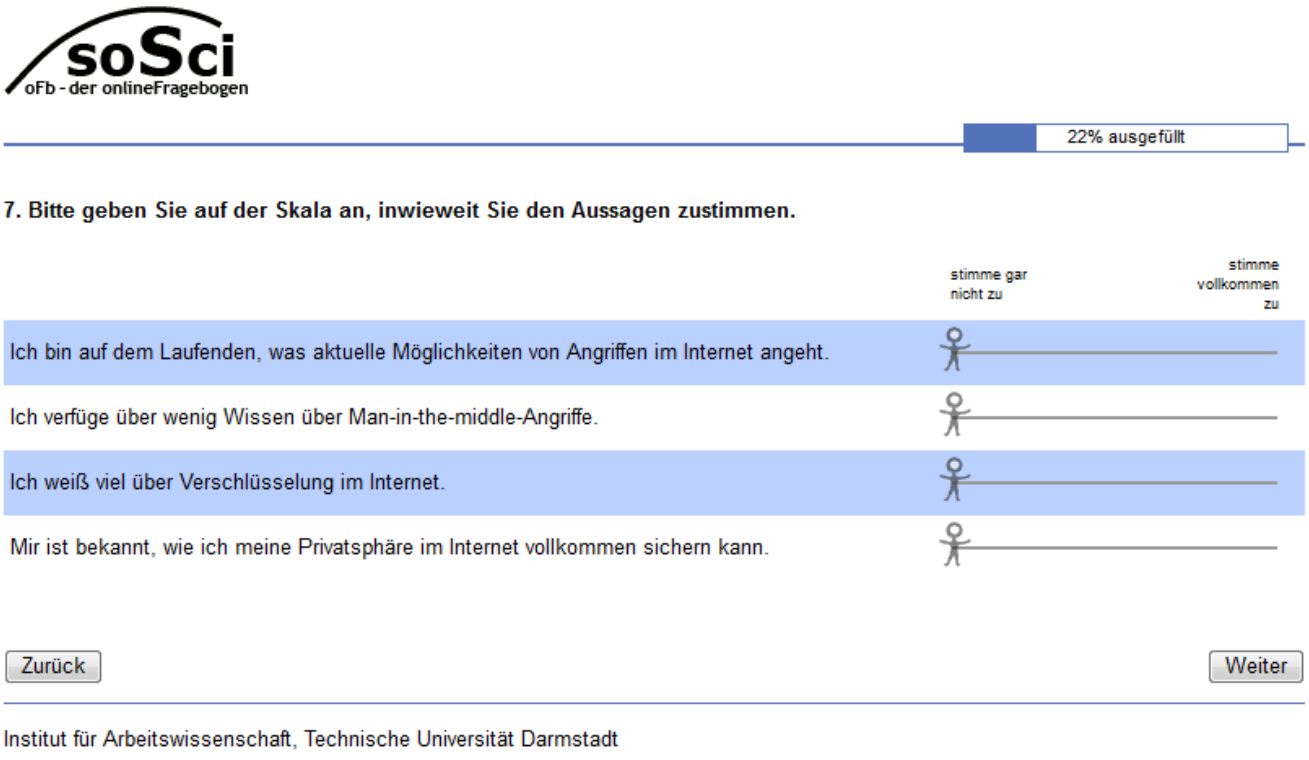
(Mehrfachnennungen möglich!)

- ☐ Desktop-PC
- ☐ Laptop/Notebook
- ☐ Tablet-PC
- ☐ Smartphone/Internetfähiges Telefon (z.B. iPhone, BlackBerry...)
- ☐ Spielekonsole (z.B. XBOX, Playstation, Game Cube...)
- ☐ keines von diesen

Zurück Weiter

Institut für Arbeitswissenschaft, Technische Universität Darmstadt

Teil 2 (nach Bearbeitung der Aufgabe)



soSci
oFb - der onlineFragebogen

33% ausgefüllt

8. Es gibt E-mails, mit denen Betrüger erreichen wollen, dass man seine persönlichen Daten preisgibt.

- stimmt
- stimmt nicht
- weiß ich nicht

9. Die einzigen Daten, die im Internet von mir gespeichert sind, sind die, die ich selbst angegeben habe.

- stimmt
- stimmt nicht
- weiß ich nicht

10. Was ist die beste Definition für Cookie?

- Etwas, das Ihren Computer vor unautorisierter Kommunikation außerhalb des Netzwerks schützt.
- Eine E-Mail, die Sie überlistet, Dieben Ihre sensiblen Daten zu geben.
- Etwas, das Webseiten auf Ihrem Computer ablegen, damit Sie bei Ihrem nächsten Besuch dieselben Informationen nicht noch einmal eingeben müssen.
- Andere Software, die Ihren Computer schützen kann.
- Etwas, das ohne Ihre Erlaubnis auf Ihrem Computer abgelegt wird und das verändert, wie Ihr Computer arbeitet.
- Etwas, das Ihren Computer überwacht und diese Information über das Internet sendet.
- Eine E-Mail, die versucht, Ihnen etwas zu verkaufen.
- Keine der genannten
- Ich habe dieses Wort zuvor gesehen, weiß aber nicht, was es für Computer bedeutet.
- Ich habe dieses Wort nie zuvor gesehen.

Zurück Weiter

Institut für Arbeitswissenschaft, Technische Universität Darmstadt

11. Was ist die beste Definition für Spyware?

- ○ Eine E-Mail, die versucht, Ihnen etwas zu verkaufen.
- ○ Etwas, das Ihren Computer vor unautorisierter Kommunikation außerhalb des Netzwerks schützt.
- ○ Andere Software, die Ihren Computer schützen kann.
- ○ Eine E-Mail, die Sie überlistet, Dieben Ihre sensiblen Daten zu geben.
- ○ Etwas, das Webseiten auf Ihrem Computer ablegen, damit Sie bei Ihrem nächsten Besuch dieselben Informationen nicht noch einmal eingeben müssen.
- ○ Etwas, das ohne Ihre Erlaubnis auf Ihrem Computer abgelegt wird und das verändert, wie Ihr Computer arbeitet.
- ○ Etwas, das Ihren Computer überwacht und diese Information über das Internet sendet.
- ○ Keine der genannten
- ○ Ich habe dieses Wort zuvor gesehen, weiß aber nicht, was es für Computer bedeutet.
- ○ Ich habe dieses Wort nie zuvor gesehen.

12. Was ist die beste Definition für Phishing?

- ○ Etwas, das ohne Ihre Erlaubnis auf Ihrem Computer abgelegt wird und das verändert, wie Ihr Computer arbeitet.
- ○ Andere Software, die Ihren Computer schützen kann.
- ○ Etwas, das Webseiten auf Ihrem Computer ablegen, damit Sie bei Ihrem nächsten Besuch dieselben Informationen nicht noch einmal eingeben müssen.
- ○ Etwas, das Ihren Computer vor unautorisierter Kommunikation außerhalb des Netzwerks schützt.
- ○ Eine E-Mail, die Sie überlistet, Dieben Ihre sensiblen Daten zu geben.
- ○ Eine E-Mail, die versucht, Ihnen etwas zu verkaufen.
- ○ Etwas, das Ihren Computer überwacht und diese Information über das Internet sendet.
- ○ Keine der genannten
- ○ Ich habe dieses Wort zuvor gesehen, weiß aber nicht, was es für Computer bedeutet.
- ○ Ich habe dieses Wort nie zuvor gesehen.

Zurück Weiter

13. Bei Unsicherheit, ob es sich um eine verschlüsselte Verbindung handelt, überprüfe ich,...

(Hier sind mehrere Antworten möglich!)

- [ ] ...ob die URL mit http:// beginnt.
- [ ] ...das SSL-Zertifikat.
- [ ] ...ob ein Schlosssymbol zu sehen ist
- [ ] ...ob der Name in der URL dem entspricht, was ich erwarte.
- [ ] ...ob ein Sicherheits-/Gütesiegel auf der Seite ist.
- [ ] weiß ich nicht

14. Ein Angreifer hört den Datenverkehr zwischen Ihrem Webbrowser und dem Webserver von Amazon ab. Welche Folgen kann das haben?

(Hier sind mehrere Antworten möglich!)

- [ ] Der Angreifer kann die E-Mail, die ich gerade abschicke, mitlesen.
- [ ] Der Angreifer gelangt an mein Passwort.
- [ ] Der Angreifer kann auf den Webserver von Amazon zugreifen.
- [ ] Angreifer können in meinem Namen bei Amazon bestellen.
- [ ] Der Angreifer kann einen Trojaner auf meinem Rechner installieren.
- [ ] weiß ich nicht

15. Ein Webshop (z.B. Amazon) zeichnet Ihr Verhalten auf seiner Webseite auf (z.B. welche Produkte Sie ansehen). Welche Folgen kann das haben?

(Hier sind mehrere Antworten möglich!)

- [ ] Angreifer können meinen Rechner manipulieren
- [ ] Nichts, was soll Amazon mit meinem Verhalten anfangen?
- [ ] Angreifer können detaillierte Rückschlüsse auf meine Persönlichkeit ziehen
- [ ] Ich bekomme Werbung, die auf mich zugeschnitten ist
- [ ] weiß ich nicht

Zurück Weiter

soSci
oFb - der onlineFragebogen

67% ausgefüllt

16. Der Datenschutz kann erhöht werden, indem man keine Cookies von Drittanbietern annimmt.

- ○ stimmt
- ○ stimmt nicht
- ○ weiß ich nicht

17. Ein Schloss-Symbol in der Adressleiste des Browsers bedeutet, dass...

(Hier sind mehrere Antworten möglich!)

- ☐ ...jede Information, die man eingibt, gesichert gesendet wird.
- ☐ ...man einen Schlüssel oder Passwort benötigt, um die Seite zu betreten.
- ☐ ...die Seite vertrauenswürdig ist.
- ☐ ...alle angezeigten Informationen gesichert übertragen wurden.
- ☐ weiß ich nicht

Zurück Weiter

Institut für Arbeitswissenschaft, Technische Universität Darmstadt

18. Sie sehen nun einige mögliche Tätigkeiten im Internet.

Geben Sie nun bitte für jede der folgenden Aussagen an, mit welcher Wahrscheinlichkeit Sie der genannten Aktivität oder Verhaltensweise nachgehen würden.

(Bitte klicken Sie dazu auf die Position auf der Skala, die das Strichmännchen einnehmen soll)

Wie wahrscheinlich ist es, dass Sie...	sehr unwahrscheinlich	sehr wahrscheinlich
...etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen?		
...vertrauliche Daten angeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt?		
...im Internet Daten angeben ohne Datenschutzerklärungen angeschaut zu haben?		

19. Menschen sehen in bestimmten Situationen ein Risiko, falls Unsicherheit hinsichtlich möglicher Ergebnisse oder Konsequenzen besteht und für Sie ‚ungünstige' Folgen auftreten können. Das Risiko wird jedoch sehr persönlich und intuitiv wahrgenommen, und wir möchten gerne erfahren, wie risikoreich Sie jede der Situationen einschätzen.

Schätzen Sie für jede der folgenden Aussagen den Risikograd ein, indem Sie auf die Stelle klicken an die Sie das Strichmännchen verschieben wollen.

Welches Risiko besteht, wenn Sie...	überhaupt kein Risiko	sehr hohes Risiko
...etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen?		
...im Internet Daten angeben ohne Datenschutzerklärungen angeschaut zu haben?		
...vertrauliche Daten angeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt?		

20. Schätzen Sie für jede der folgenden Aussagen ein, wie hoch der Nutzen ist, den Sie meinen, aus der Situation ziehen zu können.

(Bitte klicken Sie dazu auf die Position, die das Strichmännchen einnehmen soll)

Welchen Nutzen hat es für Sie, wenn Sie...	gar keinen Nutzen	großen Nutzen
...etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen?		
...vertrauliche Daten angeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt?		
...im Internet Daten angeben ohne Datenschutzerklärungen angeschaut zu haben?		

Zurück Weiter

Anhang C

Einverständniserklärung im Rahmen der Explorations- und der Validierungsstudie

IAD

IAD | Otto-Berndt-Str. 2 | D-64287 Darmstadt, Germany

Sehr geehrte Teilnehmer,

vielen Dank, dass Sie am Versuch zu Verhalten beim Online-Shopping teilnehmen. Sie leisten damit einen wichtigen Beitrag zur Forschung.
Wir möchten Sie hiermit darauf hinweisen, dass während dem Versuch Audio-, Video- und Blickbewegungsdaten von Ihnen aufgezeichnet werden. Sämtliche von uns aufgezeichnete Daten werden aber vertraulich und anonymisiert ausschließlich zu wissenschaftlichen Zwecken verwendet.

Lesen Sie sich bitte die Einverständniserklärung durch und unterschreiben sie an den markierten Stellen.

Ich bin damit einverstanden, dass Audio-, Video- und Blickbewegungsdaten von mir und meinem Verhalten aufgezeichnet werden.

Name: .....

Straße: .....

Wohnort: .....

Geb.-Datum: .....

Darmstadt, ... (Datum) ..... (Unterschrift)

Darüber hinaus bin ich einverstanden, dass das Videomaterial und andere Daten als Anschauungsmaterial für Wissenschaft und Forschung
Ja ☐ Nein ☐
sowie für weitere Forschungsarbeiten eingesetzt werden kann.
Ja ☐ Nein ☐

Ich erkläre mich dazu bereit, dass meine Kontaktdaten sowie wesentliche personenbezogenen Daten (Jahrgang, Brillenträger, Führerschein, etc.) in eine interne Probandendatenbank des IAD aufgenommen werden.

Ja ☐ Nein ☐

Darmstadt, ... (Datum) ..... (Unterschrift)

Technische Universität Darmstadt
Institut für Arbeitswissenschaft

Darmstadt University of Technology
Institute of Ergonomics

Institutsleiter | Head of Institute
Professor Dr.-Ing. Ralph Bruder

Petersenstrasse 30
D-64287 Darmstadt, Germany
Fon: +49 61 51. 16 29 87
Fax: +49 61 51. 16 27 98
sek@iad.tu-darmstadt.de
www.arbeitswissenschaft.de

TECHNISCHE UNIVERSITÄT DARMSTADT

Ihre erste Aufgabe besteht darin, im Internet auf einer Verkaufsplattform ein Produkt im Wert von 10 Euro zu wählen, das Sie auch wirklich erwerben möchten und für Sie einen persönlichen Nutzen generiert.

Wenden Sie sich bitte an den Versuchsleiter, sobald Sie damit fertig sind!

Instruktion 2

TECHNISCHE UNIVERSITÄT DARMSTADT

Ihre zweite Aufgabe ist, das von Ihnen gewählte Produkt auf einer Internetseite, auf der Sie noch keinen Account haben, zu einem möglichst günstigen Preis zu bestellen (nicht amazon.de, ebay.de, etc.).

Öffnen Sie dazu bitte eine neue Registerkarte.

Die 10 Euro Aufwandsentschädigung erhalten Sie auf jeden Fall, auch wenn das bestellte Produkt weniger als 10 Euro kostet!

Geben Sie bitte Ihrem Versuchsleiter Bescheid, sobald Sie diese Aufgabe beendet haben.

Anhang D

In Explorationsstudie untersuchte Hypothesen

Hypothese	Inhalt
Alter_1	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des tatsächlichen Wissens.
Alter_2	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des wahrgenommenen Wissens.
Alter_3	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich der Nutzungsdauer.
Alter_4	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich der Nutzungshäufigkeit.
Alter_5	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des Besitzes internetfähiger Geräte.
Alter_6	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des wahrgenommenen Risikos etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
Alter_7	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des wahrgenommenen Risikos im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.
Alter_8	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des wahrgenommenen Risikos vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
Alter_9	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des erwarteten Nutzens etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
Alter_10	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des erwarteten Nutzens im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.
Alter_11	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des erwarteten Nutzens vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
Alter_12	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich der Wahrscheinlichkeit etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
Alter_13	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich der Wahrscheinlichkeit im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.
Alter_14	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich der Wahrscheinlichkeit vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
Alter_15	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des tatsächlichen Verhaltens "etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen".
Alter_16	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des tatsächlichen Verhaltens "im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben".

Alter_17	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des tatsächlichen Verhaltens "vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt".
Alter_18	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des tatsächlichen Datenschutz-Verhaltens.

Hypothese	**Inhalt**
Geschlecht_1	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich des tatsächlichen Wissen.
Geschlecht_2	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich des wahrgenommenen Wissen.
Geschlecht_3	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich des wahrgenommenen Risikos etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
Geschlecht_4	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich des wahrgenommenen Risikos im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.
Geschlecht_5	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich des wahrgenommenen Risikos vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
Geschlecht_6	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich des erwarteten Nutzens etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
Geschlecht_7	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich des erwarteten Nutzens im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.
Geschlecht_8	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich des erwarteten Nutzens vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
Geschlecht_9	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich der Wahrscheinlichkeit etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
Geschlecht_10	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich der Wahrscheinlichkeit im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.
Geschlecht_11	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich der Wahrscheinlichkeit vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
Geschlecht_12	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich des tatsächlichen Verhaltens "etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen".
Geschlecht_13	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich des tatsächlichen Verhaltens "im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben".
Geschlecht_14	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich des tatsächlichen Verhaltens "vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung

Geschlecht_15	Die Gruppe der weiblichen und die der männlichen Probanden unterscheiden sich bezüglich des tatsächlichen Datenschutz-Verhaltens.
Geschlecht_16	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des tatsächlichen Verhaltens "im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben".
Geschlecht_17	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des tatsächlichen Verhaltens "vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung
Geschlecht_18	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des tatsächlichen Datenschutz-Verhaltens.

Hypothese	**Inhalt**
wahrg.Wissen_1	Die Gruppe der Nutzer mit niedrigem Score für wahrgenommenes Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für wahrgenommenes Wissen bezüglich des wahrgenommenen Risikos etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
wahrg.Wissen_2	Die Gruppe der Nutzer mit niedrigem Score für wahrgenommenes Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für wahrgenommenes Wissen bezüglich des wahrgenommenen Risikos im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu
wahrg.Wissen_3	Die Gruppe der Nutzer mit niedrigem Score für wahrgenommenes Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für wahrgenommenes Wissen bezüglich des wahrgenommenen Risikos vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
wahrg.Wissen_4	Die Gruppe der Nutzer mit niedrigem Score für wahrgenommenes Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für wahrgenommenes Wissen bezüglich des erwarteten Nutzens etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu
wahrg.Wissen_5	Die Gruppe der Nutzer mit niedrigem Score für wahrgenommenes Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für wahrgenommenes Wissen bezüglich des erwarteten Nutzens im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.
wahrg.Wissen_6	Die Gruppe der Nutzer mit niedrigem Score für wahrgenommenes Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für wahrgenommenes Wissen bezüglich des erwarteten Nutzens vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
wahrg.Wissen_7	Die Gruppe der Nutzer mit niedrigem Score für wahrgenommenes Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für wahrgenommenes Wissen bezüglich der Wahrscheinlichkeit etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu
wahrg.Wissen_8	Die Gruppe der Nutzer mit niedrigem Score für wahrgenommenes Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für wahrgenommenes Wissen bezüglich der Wahrscheinlichkeit im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.

wahrg.Wissen_9	Die Gruppe der Nutzer mit niedrigem Score für wahrgenommenes Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für wahrgenommenes Wissen bezüglich der Wahrscheinlichkeit vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
wahrg.Wissen_10	Die Gruppe der Nutzer mit niedrigem Score für wahrgenommenes Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für wahrgenommenes Wissen bezüglich des tatsächlichen Verhaltens "etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen)
wahrg.Wissen_11	Die Gruppe der Nutzer mit niedrigem Score für wahrgenommenes Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für wahrgenommenes Wissen bezüglich des tatsächlichen Verhaltens "im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu
wahrg.Wissen_12	Die Gruppe der Nutzer mit niedrigem Score für wahrgenommenes Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für wahrgenommenes Wissen bezüglich des tatsächlichen Verhaltens "vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt".
wahrg.Wissen_13	Die Gruppe der Nutzer mit niedrigem Score für wahrgenommenes Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für wahrgenommenes Wissen bezüglich des tatsächlichen Datenschutz-

Hypothese	**Inhalt**
tats.Wissen_1	Die Gruppe der Nutzer mit niedrigem Score für tatsächliches Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für tatsächliches Wissen bezüglich des wahrgenommenen Wissen.
tats.Wissen_2	Die Gruppe der Nutzer mit niedrigem Score für tatsächliches Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für tatsächliches Wissen bezüglich des wahrgenommenen Risikos etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
tats.Wissen_3	Die Gruppe der Nutzer mit niedrigem Score für tatsächliches Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für tatsächliches Wissen bezüglich des wahrgenommenen Risikos im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.
tats.Wissen_4	Die Gruppe der Nutzer mit niedrigem Score für tatsächliches Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für tatsächliches Wissen bezüglich des wahrgenommenen Risikos vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
tats.Wissen_5	Die Gruppe der Nutzer mit niedrigem Score für tatsächliches Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für tatsächliches Wissen bezüglich des erwarteten Nutzens etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
tats.Wissen_6	Die Gruppe der Nutzer mit niedrigem Score für tatsächliches Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für tatsächliches Wissen bezüglich des erwarteten Nutzens im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.

tats.Wissen_7	Die Gruppe der Nutzer mit niedrigem Score für tatsächliches Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für tatsächliches Wissen bezüglich des erwarteten Nutzens vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
tats.Wissen_8	Die Gruppe der Nutzer mit niedrigem Score für tatsächliches Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für tatsächliches Wissen bezüglich der Wahrscheinlichkeit etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
tats.Wissen_9	Die Gruppe der Nutzer mit niedrigem Score für tatsächliches Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für tatsächliches Wissen bezüglich der Wahrscheinlichkeit im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.
tats.Wissen_10	Die Gruppe der Nutzer mit niedrigem Score für tatsächliches Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für tatsächliches Wissen bezüglich der Wahrscheinlichkeit vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
tats.Wissen_11	Die Gruppe der Nutzer mit niedrigem Score für tatsächliches Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für tatsächliches Wissen bezüglich des tatsächlichen Verhaltens "etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen".
tats.Wissen_12	Die Gruppe der Nutzer mit niedrigem Score für tatsächliches Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für tatsächliches Wissen bezüglich des tatsächlichen Verhaltens "im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben".
tats.Wissen_13	Die Gruppe der Nutzer mit niedrigem Score für tatsächliches Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für tatsächliches Wissen bezüglich des tatsächlichen Verhaltens "vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt".
tats.Wissen_14	Die Gruppe der Nutzer mit niedrigem Score für tatsächliches Wissen unterscheidet sich von der Gruppe der Nutzer mit hohem Score für tatsächliches Wissen bezüglich des tatsächlichen Datenschutz-Verhaltens.
tats.Wissen_15	Die Gruppe der Nutzer, die das Internet seit 3 bis unter 7 Jahren nutzt unterscheidet sich von der Gruppe, die das Internet seit mehr als 10 Jahren nutzt bezüglich des tatsächlichen Datenschutz-Verhaltens.
tats.Wissen_16	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des tatsächlichen Verhaltens "im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben".
tats.Wissen_17	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des tatsächlichen Verhaltens "vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt".
tats.Wissen_18	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des tatsächlichen Datenschutz-Verhaltens.

Hypothese	Inhalt
N.-dauer_1	Die Gruppe der Nutzer, die das Internet seit 3 bis unter 7 Jahren nutzt unterscheidet sich von der Gruppe, die das Internet seit mehr als 10 Jahren nutzt bezüglich des tatsächlichen Wissen.
N.-dauer_2	Die Gruppe der Nutzer, die das Internet seit 3 bis unter 7 Jahren nutzt unterscheidet sich von der Gruppe, die das Internet seit mehr als 10 Jahren nutzt bezüglich des wahrgenommenen Wissen.
N.-dauer_3	Die Gruppe der Nutzer, die das Internet seit 3 bis unter 7 Jahren nutzt unterscheidet sich von der Gruppe, die das Internet seit mehr als 10 Jahren nutzt bezüglich des wahrgenommenen Risikos etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
N.-dauer_4	Die Gruppe der Nutzer, die das Internet seit 3 bis unter 7 Jahren nutzt unterscheidet sich von der Gruppe, die das Internet seit mehr als 10 Jahren nutzt bezüglich des wahrgenommenen Risikos im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.
N.-dauer_5	Die Gruppe der Nutzer, die das Internet seit 3 bis unter 7 Jahren nutzt unterscheidet sich von der Gruppe, die das Internet seit mehr als 10 Jahren nutzt bezüglich des wahrgenommenen Risikos vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
N.-dauer_6	Die Gruppe der Nutzer, die das Internet seit 3 bis unter 7 Jahren nutzt unterscheidet sich von der Gruppe, die das Internet seit mehr als 10 Jahren nutzt bezüglich des erwarteten Nutzens etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
N.-dauer_7	Die Gruppe der Nutzer, die das Internet seit 3 bis unter 7 Jahren nutzt unterscheidet sich von der Gruppe, die das Internet seit mehr als 10 Jahren nutzt bezüglich des erwarteten Nutzens im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.
N.-dauer_8	Die Gruppe der Nutzer, die das Internet seit 3 bis unter 7 Jahren nutzt unterscheidet sich von der Gruppe, die das Internet seit mehr als 10 Jahren nutzt bezüglich des erwarteten Nutzens vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
N.-dauer_9	Die Gruppe der Nutzer, die das Internet seit 3 bis unter 7 Jahren nutzt unterscheidet sich von der Gruppe, die das Internet seit mehr als 10 Jahren nutzt bezüglich der Wahrscheinlichkeit etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
N.-dauer_10	Die Gruppe der Nutzer, die das Internet seit 3 bis unter 7 Jahren nutzt unterscheidet sich von der Gruppe, die das Internet seit mehr als 10 Jahren nutzt bezüglich der Wahrscheinlichkeit im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.
N.-dauer_11	Die Gruppe der Nutzer, die das Internet seit 3 bis unter 7 Jahren nutzt unterscheidet sich von der Gruppe, die das Internet seit mehr als 10 Jahren nutzt bezüglich der Wahrscheinlichkeit vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
N.-dauer_12	Die Gruppe der Nutzer, die das Internet seit 3 bis unter 7 Jahren nutzt unterscheidet sich von der Gruppe, die das Internet seit mehr als 10 Jahren nutzt bezüglich des tatsächlichen Verhaltens "etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen".

N.-dauer_13	Die Gruppe der Nutzer, die das Internet seit 3 bis unter 7 Jahren nutzt unterscheidet sich von der Gruppe, die das Internet seit mehr als 10 Jahren nutzt bezüglich des tatsächlichen Verhaltens "im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben".
N.-dauer_14	Die Gruppe der Nutzer, die das Internet seit 3 bis unter 7 Jahren nutzt unterscheidet sich von der Gruppe, die das Internet seit mehr als 10 Jahren nutzt bezüglich des tatsächlichen Verhaltens "vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt".
N.-dauer_15	Die Gruppe der Nutzer, die das Internet seit 3 bis unter 7 Jahren nutzt unterscheidet sich von der Gruppe, die das Internet seit mehr als 10 Jahren nutzt bezüglich des tatsächlichen Datenschutz-Verhaltens.
N.-dauer_16	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des tatsächlichen Verhaltens "im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben".
N.-dauer_17	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des tatsächlichen Verhaltens "vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt".
N.-dauer_18	Die Gruppe der jüngeren und die der älteren Probanden unterscheiden sich bezüglich des tatsächlichen Datenschutz-Verhaltens.

Hypothese	**Inhalt**
Besitz_1	Die Gruppe der Nutzer die keine oder nur wenige internetfähige Geräte besitzen unterscheidet sich von der Gruppe der Nutzer die viele internetfähige Geräte besitzen bezüglich des wahrgenommenen Risikos etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
Besitz_2	Die Gruppe der Nutzer die keine oder nur wenige internetfähige Geräte besitzen unterscheidet sich von der Gruppe der Nutzer die viele internetfähige Geräte besitzen bezüglich des wahrgenommenen Risikos im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.
Besitz_3	Die Gruppe der Nutzer die keine oder nur wenige internetfähige Geräte besitzen unterscheidet sich von der Gruppe der Nutzer die viele internetfähige Geräte besitzen bezüglich des wahrgenommenen Risikos vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
Besitz_4	Die Gruppe der Nutzer die keine oder nur wenige internetfähige Geräte besitzen unterscheidet sich von der Gruppe der Nutzer die viele internetfähige Geräte besitzen bezüglich des erwarteten Nutzens etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
Besitz_5	Die Gruppe der Nutzer die keine oder nur wenige internetfähige Geräte besitzen unterscheidet sich von der Gruppe der Nutzer die viele internetfähige Geräte besitzen bezüglich des erwarteten Nutzens im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.
Besitz_6	Die Gruppe der Nutzer die keine oder nur wenige internetfähige Geräte besitzen unterscheidet sich von der Gruppe der Nutzer die viele internetfähige Geräte besitzen bezüglich des erwarteten Nutzens vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
Besitz_7	Die Gruppe der Nutzer die keine oder nur wenige internetfähige Geräte besitzen unterscheidet sich von der Gruppe der Nutzer die viele internetfähige Geräte

	besitzen bezüglich der Wahrscheinlichkeit etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
Besitz_8	Die Gruppe der Nutzer die keine oder nur wenige internetfähige Geräte besitzen unterscheidet sich von der Gruppe der Nutzer die viele internetfähige Geräte besitzen bezüglich der Wahrscheinlichkeit im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.
Besitz_9	Die Gruppe der Nutzer die keine oder nur wenige internetfähige Geräte besitzen unterscheidet sich von der Gruppe der Nutzer die viele internetfähige Geräte besitzen bezüglich der Wahrscheinlichkeit vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
Besitz_10	Die Gruppe der Nutzer die keine oder nur wenige internetfähige Geräte besitzen unterscheidet sich von der Gruppe der Nutzer die viele internetfähige Geräte besitzen bezüglich des tatsächlichen Verhaltens "etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen".
Besitz_11	Die Gruppe der Nutzer die keine oder nur wenige internetfähige Geräte besitzen unterscheidet sich von der Gruppe der Nutzer die viele internetfähige Geräte besitzen bezüglich des tatsächlichen Verhaltens "im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben".
Besitz_12	Die Gruppe der Nutzer die keine oder nur wenige internetfähige Geräte besitzen unterscheidet sich von der Gruppe der Nutzer die viele internetfähige Geräte besitzen bezüglich des tatsächlichen Verhaltens "vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt".
Besitz_13	Die Gruppe der Nutzer die keine oder nur wenige internetfähige Geräte besitzen unterscheidet sich von der Gruppe der Nutzer die viele internetfähige Geräte besitzen bezüglich des tatsächlichen Datenschutz-Verhaltens.

Hypothese	**Inhalt**
Risiko_1	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich des tatsächlichen Wissen.
Risiko_2	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich des tatsächlichen Wissen.
Risiko_3	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich des tatsächlichen Wissen.
Risiko_4	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich des wahrgenommenen Wissen.
Risiko_5	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich des wahrgenommenen Wissen.

Risiko_6	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich des wahrgenommenen Wissen.
Risiko_7	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich des erwarteten Nutzens etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
Risiko_8	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich des erwarteten Nutzens im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.
Risiko_9	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich des erwarteten Nutzens vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
Risiko_10	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich der Wahrscheinlichkeit etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.

Hypothese	**Inhalt**
Risiko_11	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich der Wahrscheinlichkeit im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.
Risiko_12	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich der Wahrscheinlichkeit vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
Risiko_13	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich des tatsächlichen Verhaltens "etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen".
Risiko_14	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich des tatsächlichen Verhaltens "im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben".

Risiko_15	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich des tatsächlichen Verhaltens "vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt".
Risiko_16	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich des tatsächlichen Datenschutz-Verhaltens.
Risiko_17	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich des tatsächlichen Datenschutz-Verhaltens.
Risiko_18	Die Gruppe der Nutzer mit einem niedrigen wahrgenommenen Risiko vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen wahrgenommenen Risiko bezüglich des tatsächlichen Datenschutz-Verhaltens.

Hypothese	**Inhalt**
Nutzen_1	Die Gruppe der Nutzer mit einem niedrigen erwarteten Nutzen etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen erwarteten Nutzen bezüglich der Wahrscheinlichkeit etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen.
Nutzen_2	Die Gruppe der Nutzer mit einem niedrigen erwarteten Nutzen im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen erwarteten Nutzen bezüglich der Wahrscheinlichkeit im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben.
Nutzen_3	Die Gruppe der Nutzer mit einem niedrigen erwarteten Nutzen vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen erwarteten Nutzen bezüglich der Wahrscheinlichkeit vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt.
Nutzen_4	Die Gruppe der Nutzer mit einem niedrigen erwarteten Nutzen etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen erwarteten Nutzen bezüglich des tatsächlichen Verhaltens "etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen".
Nutzen_5	Die Gruppe der Nutzer mit einem niedrigen erwarteten Nutzen im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen erwarteten Nutzen bezüglich des tatsächlichen Verhaltens "im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben".
Nutzen_6	Die Gruppe der Nutzer mit einem niedrigen erwarteten Nutzen vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt unterscheidet sich von der Gruppe der

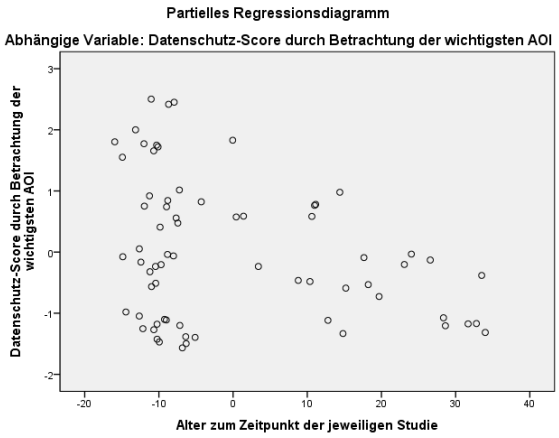
	Nutzer mit einem diesbezüglich hohen erwarteten Nutzen bezüglich des tatsächlichen Verhaltens "vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt".
Nutzen_7	Die Gruppe der Nutzer mit einem niedrigen erwarteten Nutzen etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen erwarteten Nutzen bezüglich des tatsächlichen Datenschutz-Verhaltens.
Nutzen_8	Die Gruppe der Nutzer mit einem niedrigen erwarteten Nutzen im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen erwarteten Nutzen bezüglich des tatsächlichen Datenschutz-Verhaltens.
Nutzen_9	Die Gruppe der Nutzer mit einem niedrigen erwarteten Nutzen vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt unterscheidet sich von der Gruppe der Nutzer mit einem diesbezüglich hohen erwarteten Nutzen bezüglich des tatsächlichen Datenschutz-Verhaltens.

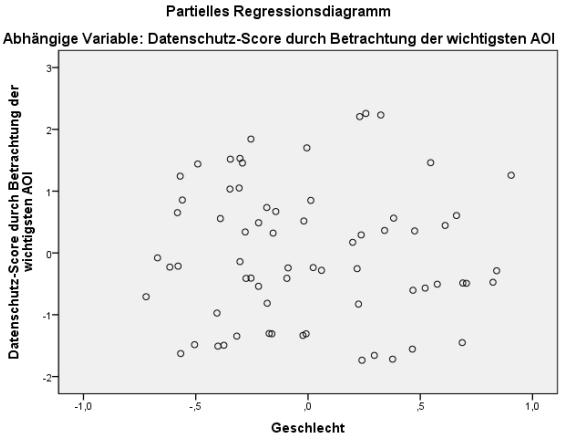
Hypothese	**Inhalt**
Wkt_1	Die Gruppe der Nutzer mit einer niedrigen angegebenen Wahrscheinlichkeit etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen unterscheidet sich von der Gruppe der Nutzer mit einer hohen angegebenen Wahrscheinlichkeit bezüglich des tatsächlichen Verhaltens "etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen".
Wkt_2	Die Gruppe der Nutzer mit einer niedrigen angegebenen Wahrscheinlichkeit im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben unterscheidet sich von der Gruppe der Nutzer mit einer hohen angegebenen Wahrscheinlichkeit bezüglich des tatsächlichen Verhaltens "im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben".
Wkt_3	Die Gruppe der Nutzer mit einer niedrigen angegebenen Wahrscheinlichkeit vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt unterscheidet sich von der Gruppe der Nutzer mit einer hohen angegebenen Wahrscheinlichkeit bezüglich des tatsächlichen Verhaltens "vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt".
Wkt_4	Die Gruppe der Nutzer mit einer niedrigen angegebenen Wahrscheinlichkeit etwas online kaufen, ohne vorher die AGB (Allgemeinen Geschäftsbedingungen) zu lesen unterscheidet sich von der Gruppe der Nutzer mit einer hohen angegebenen Wahrscheinlichkeit bezüglich des tatsächlichen Datenschutz-Verhaltens.
Wkt_5	Die Gruppe der Nutzer mit einer niedrigen angegebenen Wahrscheinlichkeit im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben unterscheidet sich von der Gruppe der Nutzer mit einer hohen angegebenen Wahrscheinlichkeit bezüglich des tatsächlichen Datenschutz-Verhaltens.
Wkt_6	Die Gruppe der Nutzer mit einer niedrigen angegebenen Wahrscheinlichkeit vertrauliche Daten anzugeben ohne sich versichert zu haben, dass es sich um eine verschlüsselte Verbindung handelt unterscheidet sich von der Gruppe der Nutzer mit einer hohen angegebenen Wahrscheinlichkeit bezüglich des tatsächlichen Datenschutz-Verhaltens.

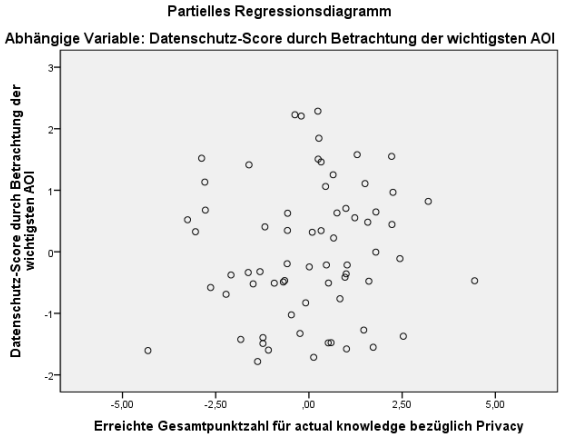
SPSS Ausgabe der Modellberechnungen zu Modell 1

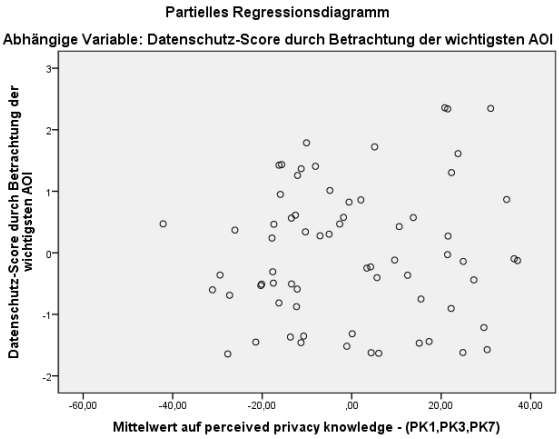
(Prädiktor: Alter, Geschlecht, wahrgenommenes und tatsächliches Wissen; Kriterium: Tatsächliches Datenschutz-Verhalten beim Onlineshopping)

E.1 Partielle Regressionsdiagramme









E.2 Durbin-Watson-Statistik

Modellzusammenfassung[b]

Modell	R	R-Quadrat	Korrigiertes R-Quadrat	Standardfehler des Schätzers	Durbin-Watson-Statistik
1	,335[a]	,112	,056	1,124	2,161

a. Einflußvariablen : (Konstante), Mittelwert auf perceived privacy knowledge - (PK1,PK3,PK7), Alter zum Zeitpunkt der jeweiligen Studie, Geschlecht , Erreichte Gesamtpunktzahl für actual knowledge bezüglich Privacy

b. Abhängige Variable: Datenschutz-Score durch Betrachtung der wichtigsten AOI

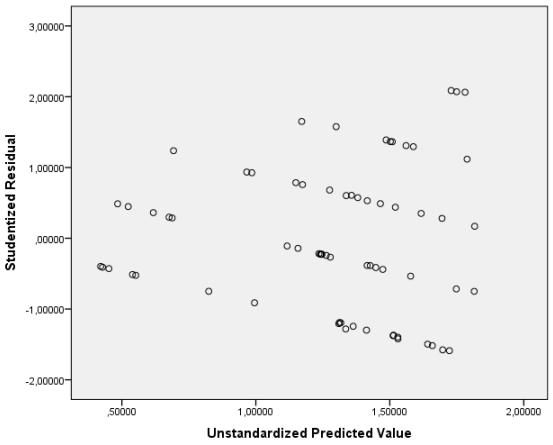
E.3 VIF=Varianzinflationsfaktor

Koeffizienten[a]

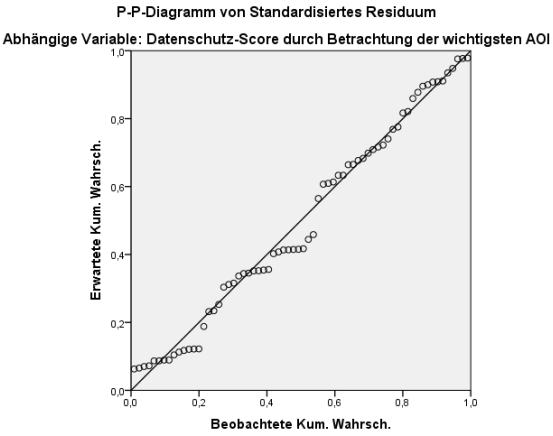
Modell		Nicht standardisierte Koeffizienten		Standardisierte Koeffizienten			95,0% Konfidenzintervalle für B		Korrelationen			Kollinearitätsstatistik	
		Regressionskoeffizient B	Standardfehler	Beta	T	Sig.	Untergrenze	Obergrenze	Nullter Ordnung	Partiell	Teil	Toleranz	VIF
1	(Konstante)	1,626	,587		2,772	,007	,454	2,798					
	Alter zum Zeitpunkt der jeweiligen Studie	-,023	,009	-,294	-2,472	,016	-,041	-,004	-,301	-,297	-,294	,997	1,003
	Geschlecht	-,055	,320	-,024	-,173	,863	-,695	,584	,064	-,022	-,021	,759	1,317
	Erreichte Gesamtpunktzahl für actual knowledge bezüglich Privacy	,062	,082	,108	,765	,447	-,101	,225	,141	,096	,091	,706	1,416
	Mittelwert auf perceived privacy knowledge - (PK1, PK3,PK7)	,004	,007	,077	,574	,568	-,010	,018	,130	,072	,068	,779	1,283

a. Abhängige Variable: Datenschutz-Score durch Betrachtung der wichtigsten AOI

E.4 Streudiagramm der Residuen



E.5 P-P-Plot



E.6 Modellberechnung lineare Regression

Modellzusammenfassung[b]

Modell	R	R-Quadrat	Korrigiertes R-Quadrat	Standardfehler des Schätzers	Durbin-Watson-Statistik
1	,335[a]	,112	,056	1,124	2,161

a. Einflußvariablen : (Konstante), Mittelwert auf perceived privacy knowledge - (PK1,PK3,PK7), Alter zum Zeitpunkt der jeweiligen Studie, Geschlecht , Erreichte Gesamtpunktzahl für actual knowledge bezüglich Privacy

b. Abhängige Variable: Datenschutz-Score durch Betrachtung der wichtigsten AOI

ANOVA[a]

Modell		Quadratsumme	df	Mittel der Quadrate	F	Sig.
1	Regression	10,060	4	2,515	1,990	,107[b]
	Nicht standardisierte Residuen	79,631	63	1,264		
	Gesamt	89,691	67			

a. Abhängige Variable: Datenschutz-Score durch Betrachtung der wichtigsten AOI

b. Einflußvariablen : (Konstante), Mittelwert auf perceived privacy knowledge - (PK1,PK3,PK7), Alter zum Zeitpunkt der jeweiligen Studie, Geschlecht , Erreichte Gesamtpunktzahl für actual knowledge bezüglich Privacy

E.7 Modellberechnung schrittweise Regression

Modellzusammenfassung[b]

Modell	R	R-Quadrat	Korrigiertes R-Quadrat	Standardfehler des Schätzers
1	,301[a]	,090	,077	1,112

a. Einflußvariablen : (Konstante), Alter zum Zeitpunkt der jeweiligen Studie

b. Abhängige Variable: Datenschutz-Score durch Betrachtung der wichtigsten AOI

ANOVA[a]

Modell		Quadratsumme	df	Mittel der Quadrate	F	Sig.
1	Regression	8,109	1	8,109	6,560	,013[b]
	Nicht standardisierte Residuen	81,582	66	1,236		
	Gesamt	89,691	67			

a. Abhängige Variable: Datenschutz-Score durch Betrachtung der wichtigsten AOI

b. Einflußvariablen : (Konstante), Alter zum Zeitpunkt der jeweiligen Studie

Koeffizienten[a]

Modell		Nicht standardisierte Koeffizienten		Standardisierte Koeffizienten		
		Regressionskoeffizient B	Standardfehler	Beta	T	Sig.
1	(Konstante)	2,081	,341		6,107	,000
	Alter zum Zeitpunkt der jeweiligen Studie	-,023	,009	-,301	-2,561	,013

a. Abhängige Variable: Datenschutz-Score durch Betrachtung der wichtigsten AOI

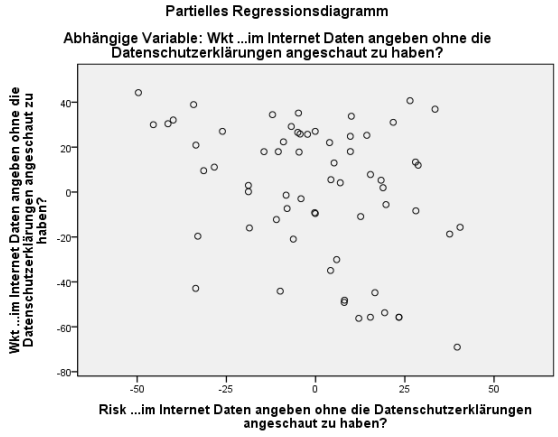
Anhang F

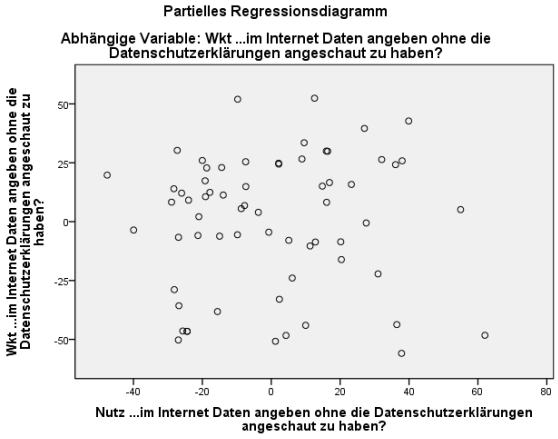
SPSS Ausgabe der Modellberechnungen zu Modell 2

(Prädiktoren: *wahrgenommenes Risiko im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben* und *erwarteter Nutzen im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben; Kriterium: Wahrscheinlichkeit im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben*)

Multiple logistische Regression

F.1 Partielle Regressionsdiagramme





F.2 Durbin-Watson-Statistik

Modellzusammenfassung[b]

Modell	R	R-Quadrat	Korrigiertes R-Quadrat	Standardfehler des Schätzers	Durbin-Watson-Statistik
1	,352[a]	,124	,096	29,324	1,831

a. Einflußvariablen : (Konstante), Nutz ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?, Risk ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?

b. Abhängige Variable: Wkt ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?

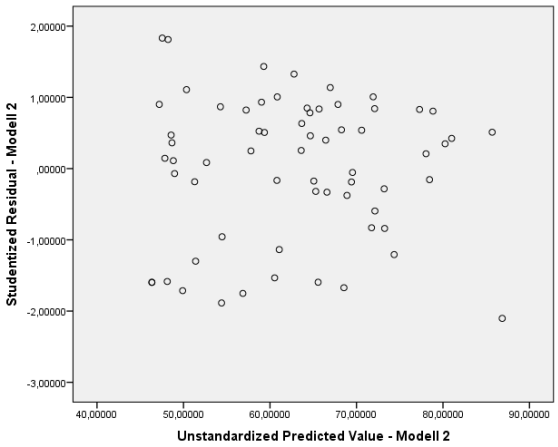
F.3 VIF=Varianzinflationsfaktor

Koeffizienten[a]

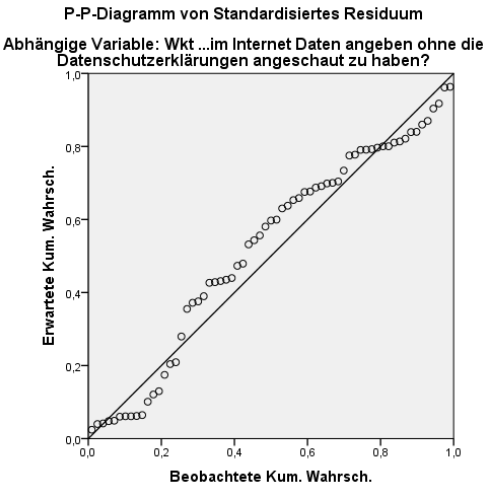
Modell		Nicht standardisierte Koeffizienten		Standardisierte Koeffizienten			95,0% Konfidenzintervalle für B		Korrelationen			Kollinearitätsstatistik	
		Regressionskoeffizient B	Standardfehler	Beta	T	Sig.	Untergrenze	Obergrenze	Nullter Ordnung	Partiell	Teil	Toleranz	VIF
1	(Konstante)	91,254	14,261		6,399	,000	62,748	119,761					
	Risk ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?	-,445	,164	-,338	-2,717	,009	-,773	-,118	-,350	-,326	-,323	,913	1,095
	Nutz ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?	,051	,152	,041	,333	,741	-,253	,354	,141	,042	,040	,913	1,095

a. Abhängige Variable: Wkt ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?

F.4 Streudiagramm der Residuen



F.5 P-P-Plot



F.6 Modellberechnung multiple Regression

Modellzusammenfassung[b]

Modell	R	R-Quadrat	Korrigiertes R-Quadrat	Standardfehler des Schätzers	Durbin-Watson-Statistik
1	,352	,124	,096	29,324	1,831

a. Einflußvariablen : (Konstante), Nutz ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?, Risk ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?

b. Abhängige Variable: Wkt ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?

ANOVA[a]

Modell		Quadratsumme	df	Mittel der Quadrate	F	Sig.
1	Regression	7558,207	2	3779,103	4,395	,016[b]
	Nicht standardisierte Residuen	53314,731	62	859,915		
	Gesamt	60872,938	64			

a. Abhängige Variable: Wkt ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?

b. Einflußvariablen : (Konstante), Nutz ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?, Risk ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?

Koeffizienten[a]

Modell		Nicht standardisierte Koeffizienten		Standardisierte Koeffizienten			95,0% Konfidenzintervalle für B		Korrelationen			Kollinearitätsstatistik	
		Regressionskoeffizient B	Standardfehler	Beta	T	Sig.	Untergrenze	Obergrenze	Nullter Ordnung	Partiell	Teil	Toleranz	VIF
1	(Konstante)	91,254	14,261		6,399	,000	62,748	119,761					
	Risk ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?	-,445	,164	-,338	-2,717	,009	-,773	-,118	-,350	-,326	-,323	,913	1,095
	Nutz ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?	,051	,152	,041	,333	,741	-,253	,354	,141	,042	,040	,913	1,095

a. Abhängige Variable: Wkt ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?

F.7 Logistische Regression (Einschluss)

(Prädiktoren: *Risiko, Nutzen* und *Wahrscheinlichkeit im Internet Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben;* Kriterium: *Tatsächliches Verhalten bezüglich Daten anzugeben ohne die Datenschutzerklärungen angeschaut zu haben*)

Variablen in der Gleichung

		Regressionskoeffizient B	Standardfehler	Wald	df	Sig.	Exp(B)	95% Konfidenzintervall für EXP (B)	
								Unterer Wert	Oberer Wert
Schritt 1[a]	Risk ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?	-,014	,014	1,046	1	,306	,986	,959	1,013
	Nutz ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?	,010	,012	,603	1	,437	1,010	,986	1,034
	Wkt ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?	,008	,011	,572	1	,449	1,008	,987	1,030
	Konstante	-1,019	1,492	,466	1	,495	,361		

a. In Schritt 1 eingegebene Variablen: Risk ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?, Nutz ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?, Wkt ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?.

F.8 Punktbiseriale Korrelation

Korrelationen

		Wkt ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?	Infos zu DS angeschaut oder nicht
Wkt ...im Internet Daten angeben ohne die Datenschutzerklärungen angeschaut zu haben?	Korrelation nach Pearson	1	,086
	Signifikanz (2-seitig)		,472
	N	73	73
Infos zu DS angeschaut oder nicht	Korrelation nach Pearson	,086	1
	Signifikanz (2-seitig)	,472	
	N	73	73